N00228-85-G-3323

DESIGNING FOR SECURITY: PROTECTING OUR SHORE FACILITIES FROM THE TERRORIST THREAT

BY

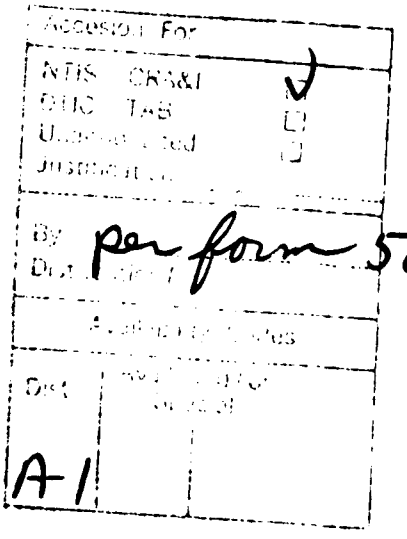
EUGENE F. HUBBARD

A REPORT PRESENTED TO THE GRADUATE COMMITTEE
OF THE DEPARTMENT OF CIVIL ENGINEERING IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF ENGINEERING

UNIVERSITY OF FLORIDA

Spring 1988

I would like to dedicate this paper to my two children, who put up with me studying and working at night and weekends as well as during the week. I would especially like to acknowledge the patience and help of my wife, Doretta, who, despite going through a pregnancy and the added burden of a new baby, supported my efforts fully and who always found the time to proof read my term papers. I would also like to thank Professor W.G. Shafer for his guidance throughout my pursuit for the M.E. degree and to the Naval Civil Engineering Laboratory for all their assistance in providing material and contact points for this paper.



"I declare that we shall train them for terrorist and suicide missions and allocate trainers for them and place all the weapons needed for such missions at their disposal."

-Muammer el-Qaddafi
Tripoli, January 15, 1986
New York Times

"The one means that wins the easiest victory over reason: terror and force."

-Adolf Hitler
Mein Kempf[1]

TABLE OF CONTENTS

CHAPTER 1

TERRORISM

1.1 Introduction

International terrorism has become the major threat to our shore facilities in the 1980's. Terrorist attacks have damaged American buildings and killed and injured American personnel, both military and civilian. One way to counter the increasing terrorist threat is to design our facilities to minimize damage resulting from a terrorist attack. This paper will focus on some of the design and structural methods that can be used to protect a facility from a terrorist attack.

Terrorism is on the rise. The number of terrorist attacks has increased almost every year from the early 1970's to the present. Although there were some years when the total number of terrorist incidents did not rise significantly, the number of casualties and amount of damage resulting from those attacks did increase during those years. In other words, the severity of terrorist attacks is rising at least as fast as the shear number of attacks.

From 1970 to 1984 there were more than 23,000 terrorist incidents that left more than 41,000 dead and 24,000 wounded. According to Dr. Ikle (Under Secretary of Defense), terrorism increased more than 40% in 1983 to a total of over 700 attacks. The estimates for 1986

and future years are for international terrorism to continue to increase to over 800 incidents per year.

The United States is a target for many terrorist acts. Since 1969, terrorists have killed or wounded over 1000 Americans. Fifty percent of terrorism in the 1980's is directed towards American facilities[2]. Who can forget the 1983 bombings of the American embassy and marine barracks in Beirut with combined deaths of over 250? The many kidnappings in the Middle East, the hijackings of the Achille Lauro and TWA Flight 847 in 1985 each resulting in the death of one American, and the numerous other bombings and attacks on embassies, restaurants, nightclubs and other targets throughout the world, are evidence of the rising tide of terrorism. Even as recently as December, 1987, the USO club in Barcelona, Spain was attacked by a lone terrorist with a hand grenade causing yet another American casualty due to terrorism. As one author put it, "Welcome to World War III."[3]

Thus, the rise of terrorism is a serious threat to American interests overseas. It is necessary for the United States to take defensive measures to protect its overseas facilities from damage and loss of life. This paper will concentrate on the design and construction options available to help counter the terrorist threat, especially structural and perimeter defenses.

1.2 The Definition of Terrorism

Terrorism is not easy to define but there are many aspects of terrorism that are common in most definitions. There is, however, still a fine line between terrorism and guerilla warfare.

One definition of terrorism was offered by Dr. Ray Cline as "the deliberate employment of violence or threat of the use of violence to commit acts in violation of law for the purpose of creating overwhelming fear in a target population larger than the number of victims attacked or threatened."[4] This definition, with some minor modifications, has been used by many others to define terrorism as simply as possible.

However, terrorism is not simple. What differentiates the terrorist from the soldier? Is a lone gunman who takes a store clerk hostage a terrorist? There are several attributes of terrorism that set it aside as a special category of crime and warfare.

First, the terrorist target almost always consists of innocents. Terrorists seldom attack an opposing force in a direct confrontation as would occur between soldiers in a battle or war. Military personnel are often the target of terrorism, such as the Marine barracks in Beirut, but the attacks are not carried out during a time of declared war with the target.

Guerillas and soldiers wage war on soldiers and, unlike most terrorist acts, do not kill civilians or neutral soldiers as an objective. This is not to say that innocent civilians are not often casualties of war, declared or guerilla, but that they are usually undesired casualties, whereas the terrorist will target civilians specifically.

Terrorism involves a willingness to commit crimes and use violence to shock, stun or intimidate a target group. The objective of the terrorist is to obtain some political or idealogical goal by creating social conflict or unrest. Their overall goal is to use isolated violent attacks to influence or destabilize a government. Their specific goals vary widely from simply disrupting or discrediting governments or other groups to formation of a new government or country.

From the above attempt to define terrorism, it can be seen that terrorism is not always easy to nail down. What one group of people may consider terrorism, another may consider guerilla warfare with legitimate goals. Guerilla groups and armies can commit terrorist acts even though they may not technically be referred to as a terrorist organization. The one common thread running through all definitions of terrorism is the willingness to use violence against innocents and neutrals. This violence is increasing in magnitude.

1.3 The Terrorist Threat

The previous sections defined terrorism and indicated the need to protect facilities from terrorist attack. Before an engineer can design a defense, however, he must have some indication of what the threat might be.

In addition to the number of attacks increasing, the violence of each attack is also increasing. The weapons of the terrorist are becoming more sophisticated, efficient and deadly. Attacks can often be launched from considerable distances or concealed weapons can be easily snuck into the target area. If one objective of terrorism is to instill fear in a target populace, then the terrorist will use whatever weapon is required to cause the most damage and death possible. This means that hijackings and kidnappings that resulted only in fleeting press attention are losing the appeal they once had. Bombings and assassinations have taken the forefront of the terrorist arsenal, and these tactics do result in more death.

The weapon of choice among terrorists today is the bomb. The types of bombs used vary and a bomb may take hundreds of different forms. Bombs vary from the letter or shopping bag bomb, which is normally used to kill a specific individual, to the car bomb, which can be used to kill specific targets and/or damage facilities. The

defense against a bomb will also vary with the bomb type. It should be noted that bombs can be detonated in a number of different ways, from contact to fuses operated by handling the bomb (i.e., the letter bomb) to remote control fuses. Bombs can also be shaped by using plastic explosives to resemble almost any common object, such as a briefcase[5].

Another common weapon used by terrorists is small arms. The developement of new types of small arms continues with such innovations as the all-plastic gun which can avoid detection by metal detectors. Small arms ammunition has also advanced to the advantage of the terrorist. For example, KTW (Teflon-coated) armor-piercing bullets, the "black steel projectile", and rapid energy armor piercing rounds have all been found in terrorist stocks[6]. Small arms and ammunition are readily available and inexpensive to terrorist groups.

Stand-off weapons, including mortars, portable rockets and missiles and rocket propelled mortars have become increasingly popular with terrorists, especially with the willingness of some state sponsers to provide them. These weapons are extremely dangerous to personnel and facilities and are popular with terrorists for both their destructive potential and their stand-off feature. The terrorist does not need to expose himself when using these weapons.

Perhaps the most dangerous terrorist weapon is a chemical, biological or nuclear device. The potential for damage to personnel, facilities and the economy by use of one of these weapons is unimaginable. There is increasing evidence that these weapons are becoming available to terrorists. Since the only real defense against these types of weapons is to control the availability of the weapon itself, a monumental if not impossible task, they will not be discussed in this paper. Sooner or later, however, a terrrorist group may hold a whole city, and thus a nation, hostage with a nuclear device.

As technology increases so will the effectiveness and deadliness of terrorist weapons. They will become harder to detect and more difficult to defeat. This makes the job of the engineer trying to design to protect facilities from the terrorist threat more difficult and more important. As terrorists obtain newer, more advanced weapons, new defenses must be developed to counter the threat.

There are a few developments in modern day terrorism that the design engineer should be aware of to determine the scope of the threat. First is the rise of state terrorism. Several countries are known to actively support, encourage, fund and supply terrorism. Countries such as Iran, Syria, Lybia, Nicaraugua, Cuba,

East Germany, the Soviet Union, North Korea and many others support terrorism in some direct manner. This is one method for a terrorist group to obtain the weapons described above. State supported terrorism is on the rise, posing a serious threat to possible targets*.

Terrorist groups are also joining together to support one another. What may be the worst recent terrorism developement is evidence that many terrorist groups, especially those operating in South America, such as the Shining Path group, and the Middle East, such as the Amal, the PLO and the Islamic Jihad, are now joining forces with drug smuggling organizations. Terrorist groups acting together or with other illegal organizations double the threat and increase the level of violence that may be used by these groups. Money from drug operations help to finance weapons purchases. There is evidence now that terrorist groups are moving into the drug smuggling business to finance their organizations. By doing this, some organizations may move away from their original idealogical goals and towards a profit goal. Although that may reduce their attacks against innocents, new drug smuggling operations are just as undesirable as fanatical terrorist organizations. In the United States, there is also growing evidence that domestic and foreign terrorist groups are joining with street gangs to gain entrance into the profitable U.S. drug trade.

1.4 Responses to Terrorism

There are many methods available to try to fight terrorism. The responses typically fall into the political arena, legal areas, military/counter-attack options, and defensive options. This paper will deal with the defensive options but the other responses do merit brief attention.

Politically, the options to combat terrorism are numerous. The largest single factor is cooperation between nations. Pressure must be put on all state sponsors of terrorism from all other countries. Intelligence must be shared among nations. Terrorism of all forms should be condemned by all concerned. This will not be easy but should be a primary goal of the United States, the #1 target of terrorism.

Legally, laws can be passed in the United States that can help to prosecute terrorists and prevent terrorist acts from occurring in the United States. The main hurdle in the legal area is the definition of terrorism. Congress has passed laws such as Public Law 98-473 that makes it a crime to siege, detain, threaten to kill or otherwise commit terrorist acts against Americans. Public Law 98-533 offers a $500,000 reward for information leading to the arrest of terrorists. But a law making it illegal for American individuals or businesses to support terrorism has not been passed due

to confusion about the definition of terrorism. Many Americans feel it is their right to support "guerilla" groups such as the Irish Replubican Army, the Palistinian Liberation Organization, the Contras, African National Congress and others. The distinction between these "political" groups and terrorists can be a fine line.

Another option for the United States is to mount a counter-attack or retaliatory strike. The use of military force to deter terrorism is a controversial issue. The main problem for the United States in using military strikes is ensuring that the attack is directed at the right target. In other words, before a retaliatory strike can be staged, the perpetrators of the terrorist act or their sponsors must be clearly identified. Otherwise, innocents may be attacked, which would cause even more anti-American feelings among the countries involved. The Reagan administration did launch a counter-strike on Lybia shortly after a bomb exploded in a West German nightclub that is frequented by American servicemen. A commercial airliner carrying the terrorists involved in the hijacking of the TWA flight and killing of an American serviceman was intercepted by U.S. fighters and forced to land in Italy, where they were promptly arrested.

There are many other responses to terrorism that can

be taken by the United States, but the effectiveness of any of them is questionable. The political process can be long and requires cooperation and agreement from countries that may never be willing to give it. The legal options have the same problem, lack of cooperation, plus lack of recognition of international laws and U.N. authority, along with the problem of legally defining terrorism and separating it from legitimate political groups. The military options can be a viable deterrence to terrorism but has the problem of identifying the targets. Most other responses have similar problems and no action is likely to eliminate terrorism completely[9].

Democratic societies, such as the United States, are particularly vulnerable to terrorist attacks. Even if the government of a democracy is ready to use force against terrorists, the actions may be met with resistance from the general public, the voters. If a democratic country is attacked itself, thus far a rarity in the United States, and the government has to resort to such methods as martial law to combat it, then the terrorists have succeeded in one of their goals, disrupting the government and causing dissent in the general populace. The structure of a democratic government and the ideas on which democracy is based, i.e. freedom, make it an ideal target for terrorism.

So what can the United States do? It should follow all of the above responses and pursue covert actions against terrorists. However, protection of likely targets should have a high priority. Terrorism will be around for a long time, designing our facilities to reduce its effects is one action the United States can take *now* to combat and deter terrorists.

CHAPTER II

DESIGN CONSIDERATIONS

2.1 The Threat Analysis

Before an engineer can begin to design a facility that is a possible target for terrorists, the probability of terrorist attack, the terrorists that may be involved and the type of weapons likely to be used should be identified or assumed. These criteria are most often evaluated at the beginning of the design cycle by developing a threat analysis. Although the designer is not often responsible for developing the threat analysis, he should be aware of how it is being prepared and who is involved in its preparation. This will allow the designer to adequately determine the best way to protect the facilities under design.

Some of the items that should be included in the threat analysis are:

1. Terrorist groups active in the area including the number of groups, number of members, goals of each group, methods normally employed by each group and type of target attacked by each group.

2. The type of weapons available and used by terrorists who may attack the facility under design.

3. The estimated probability of attack on the particular facility.

4. The local law enforcement agencies that can deter or prevent an attack or provide assistance in the case of an attack.

5. The local political climate, especially in regards to their support or resistance to terrorism.

All of the above items and more can assist planners in determining what level of protection should be designed into the facility.

The preparation of the threat analysis should be a team effort. Members of the team include the following: the customer or his representative (the Commanding Officer in the case of a military facility); security specialists; members of various law enforcement agencies, especially those knowledgeable with local threats and local law enforcement capabilities; the designer; and anyone else who has an important interest in the project or special knowledge of the threat.

The designer and physical security specialists are important members of the threat analysis team. They can identify design options to meet the threat early on in the process and the associated costs of each option. They can also assist in evaluating the damage and loss of life that might occur should a specific attack be launched.

The team involved in preparing the threat analysis is an extension of the design team. The differences between the design team, as discussed below, and the

threat analysis team is in the area of specialists. The threat analysis requires members with law enforcement and intelligence backgrounds who are knowledgeable with terrorist activities. The design team specialists include the appropriate engineering disciplines (i.e., electrical, structural, mechanical, security, etc.). However, in a long term project, law enforcement, intelligence and security personnel should be consulted often as the political climate and terrorist activities in many areas are constantly changing.

Computer simulation has become useful in evaluating the threat. Many programs are now available that will give a threat analysis with various inputs.

2.2 The Design Team

The design team involved in designing a project with physical security as a priority can be a little more complex than the normal design team. Once the threat has been determined and reported in the threat analysis, the design team must determine what to protect, type of protection desired, amount of protection necessary and type and degree of damage that can be considered acceptable. The answers to these questions must then be used as a basis for the security design.

The security design team should include representatives from operations (the users of the

system), security, support services and administration along with the architects/engineers. The users, or customer, have proven invaluable on design teams in helping to design specific security systems[11]. The design team should include strong command/management involvement to ensure that security needs do not override other desires, such as aesthetics and functional use, that may also be considered important.

Once the security analysis is complete, the next step is to perform a security, or vulnerability, assessment. The security assessment will determine what resources are already in existence at the project site and what additional requirements must be met. It should be kept concise and simple and should identify the following:

-Mission of the facility;

-Site assessment;

-Risk analysis and reduction;

-Personnel and vehicle access requirements;

-Physical and electronic security sytems necessary;

-Security forces requirements.[12]

From the above, the design team can now begin the actual design of a secure facility.

2.3 What to Protect

"You can have perfect physical security and still be penetrable by visa applicants and garbage collectors."

-Yehiel Fromer
President, Slocoor, Inc.[19]

A major part of the design team efforts early on will be to decide what should be protected. Should the whole project be protected or just a part of it? The amount of protection finally decided on will be a function of the threat and of the amount of funds available. A cost versus loss analysis should be completed to determine exactly how much protection can be provided.

The designer will have to provide protection in many areas of the project. Structurally, the walls, roofs and floors, windows and doors may all require hardening or some other form of protection. Perimeter defense can be especially important against terrorist attack.

Protection of specific structures and perimeter defense are both important, but the designer must not forget to protect utility systems. Utilities, especially water and power, must be protected from destruction or disruption. Utility tunnels facilitating sewers, ventilation systems, etc., also have to be

designed so as not to afford a terrorist access to the facility. There are many methods available to accomplish structural, perimeter and utility protection.

2.4 How To Protect

> "The White House today looks imprisoned in its own ring of concrete. This does not have to be. Good engineering and good security are not mutually exclusive."
> -Robert Messmer[14]
> Senior Vice President
> Hellmuth, Obata and Kasssabaum, Inc.

Once the design team has determined what buildings, or parts of buildings, must be protected from terrorist acts, the next question that must be answered is how to protect those facilities. The type and amount of physical security systems necessary must be determined. Different options should be prepared and compared. Deciding on what security options to use will then lead into the actual design of the facility.

The type and amount of protection used will be dependent on several factors, including the probability of attack and method of attack and the cost of the security system. The estimated cost of the loss incurred from a terrorist attack, taking into account the probability of an attack, must be weighed against the estimated cost of providing necessary security. This type of analysis, standard in almost any design, should result in an economical security system.

The options available for protecting a facility against an attack are numerous. Specific construction methods and materials can harden a facility. The selection of the facility site is very important from a security standpoint. Perimeter defense involves electronic measures, fences, barriers and guards. Access to the facility can be controlled at the perimeter by guards and barriers and at the structure by guards and electronic identification or monitoring systems.

All of the above options will be discussed in more detail in the following chapters.

2.5 Design Procedures

The following is a summary of the design procedure for a facility where probability of terrorist attack is high. Some specifics of some of the more unique design steps were discussed above. Appendix D contains a description of a program used for security design, the Physical Requirements Assessment Methodology (PSRAM).

SUMMARY OF SECURITY DESIGN

1. PLANNING STAGE:

   -Define requirements;
   -Define general scope;
   -Feasibility study;
   -Threat Analysis;
   -Preliminary site selection.

2. PRELIMINARY DESIGN:

   -Develop initial drawings
    and specifications;
   -Conduct vulnerability assessment;
   -Determine what needs to be protected;
   -Determine acceptaple losses;
   -Develop initial security design;
   -Determine cost estimates.

3. FINAL DESIGN:

   -Determine final security systems required to
    meet the threat with the funds available;
   -Prepare final drawings and specs;
   -Develop schedules.

4. ADVERTISE AND AWARD CONTRACT

5. FOLLOW-UP:

   -Check installation and operation of security
    and integrated systems to ensure operability,
    maintainability etc.

OVERALL GOAL OF DESIGN: Produce the best security system for the lowest cost possible.

CHAPTER III

PERIMETER DEFENSE

3.1 Layered Defense

The first line of defense for most facilities will be its perimeter. There are a number of ways to protect a facility by protecting the exterior grounds around the facility. A layered defense, including siting considerations, electronic measures, access control, vehicle barriers and blast barriers, is probably the best means of protecting a facility.

The objective of perimeter defense is to deter or prevent an attacker from reaching the critical facility. If a good perimeter security system is designed, the facility may not require as much structural protection, which can get expensive.

3.1.1 Site Selection

An important consideration in the design of a secure facility is its site selection. Planners should keep security in mind as much as possible when considering the site for a possible terrorist target. If the site location is dictated by other factors, the security engineer can possibly improve the site conditions to make it more secure.

Considerations in the siting of the building include the location of trees, streams, embankments, etc. It is possible to use the terrain to help provide perimeter security. For example, trees, embankments and streams can act as vehicle barriers. However, natural terrain can also aid the terrorist. For example, a wooded area near a facility can provide cover for an attacker.[13]

Location of the building or buildings within the site is also important. The building should be located as far away from the perimeter as possible. This will aid in the design of exterior security and increase the delay time of an attacker. It also allows for a large enough stand-off distance should a vehicle bomb explode against a vehicle barrier. The building location can also be influenced by the natural terrain of the site. The building should be observable by the security forces and guards that are protecting it. Thus, buildings should not be located over hills or behind trees or embankments that may obscure it from view from guards.[14]

Terrain can therefore work for or against the security of the building. The security engineer can take advantage of certain site features but must also deal with those features that may actually aid the terrorist. Figure 3.1 shows some terrain features that must be considered.

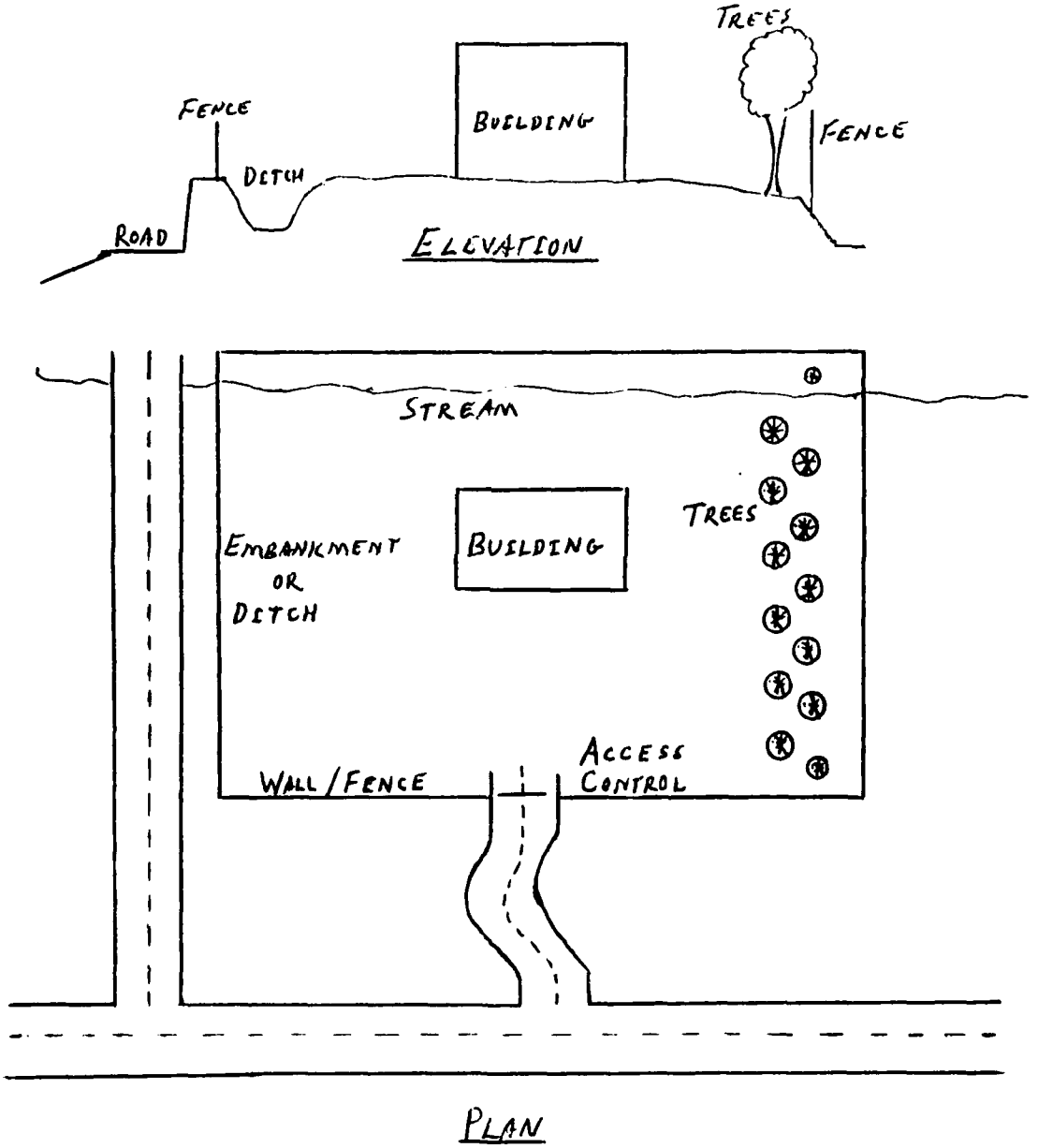


Figure 3.1: Use of Site Planning for Protection from Terrorist Attack

Clear zones should also be provided around the building or perimeter. Clear zones usually consist of a 20 to 100 foot strip that is kept mowed and is cleared of obstructions so that unusual activity around the perimeter can be observed. In the Navy, clear zones are required to be maintained.[17]

3.1.2 Access Control

Limiting access to a compound or building is one effective means of reducing the threat. Access control usually consists of issuing identification (ID) cards and using guards to check the ID cards. Proper access control that uses guards requires that the guards be well trained in their duties and in spotting counterfeit ID's.

If guards are used to provide access control at perimeter gates, design of the guardhouses, lights and ingress/egress routes also become important. A lone sentry standing out in the open is not much of a deterrent to a terrorist and it is almost impossible for a single guard armed with a small weapon to stop a speeding car. Placement of vehicle barriers can aid a guard in slowing or stopping a vehicle. Instead of entrance roads being straight, putting in curves can slow a vehicle down significantly. The guardhouse should be protected from both small arms fire and

ramming vehicles and it should be well lit. Many of the structural security options discussed in this paper should be considered for the guardhouses.

The importance of a trained and alert guard force cannot be over-emphasized. Even if the many electronic countermeasures and detection devices are used, guards are often still a key element in the facility's defense.[18]

Another means of providing access control is by installing an electronic card control system. These systems usually employ cards with magnetic coded strips that are read by a special card reader. Access is then automatically granted to the card holder. The major fault with this system is that cards can be stolen. Access is actually granted to the card, not to the specific individual. Other electronic systems are being developed which use unique individual characteristics, such as fingerprints, eye retinae, or even voice pattern recognition, to grant access.[19] These systems can be used at perimeter entrances through gates or main building or space entrances.

3.1.3 Fencing

Fencing will provide only a minor amount of protection against a terrorist attack. Most types of fences are easily broached by a well-equipped terrorist. However, fencing, in combination with proper lighting,

clear zones, intrusion detection devices and guards, can provide what could be a crucial period of delay time for an attacker.

Standard chain link fences offer less than 2 minutes of penetration time (the time for an average intruder to create a man-sized opening). However, they can be reinforced, or hardened, to offer the appearance of greater resistance, thus becoming a deterrent. Fences can be hardened with cables that are anchored to strong posts, such as concrete posts. These cables can provide a measure of protection for a vehicle that may try to crash through the fence. The penetration distance of such fences has been measured by the Naval Civil Engineering Laboratory (NCEL) at 7 to 26 feet.[2] However, if vehicle bombs are the threat, fences are not effective barriers. Vehicle barriers are discussed in more detail in section 3.3.

The other options for hardening fences consist mainly of different configurations of fencing and barbed wire. Many combinations of fencing, barbed wire and concertina (rolled) barbed tape are used, with the barbed wire on top of the fence or along the bottom, or a combination of both (see figure 3.2). Since standard fencing options will do little to stop a terrorist, the fence should be augmented with some other form of barrier, such as concrete bollards, ditches, streams,

walls, etc. Lighting and intrusion detection devices can also augment fencing. The height of a fence has proven to add only a few seconds to penetration time. Fabric tie-downs can be used to discourage entrance by going under the fence.

3.1.4 Lighting

Lighting is important to physical security for a number of reasons. Many attacks occur at night under the cover of darkness. Perimeter lighting can remove most of the advantage of a nighttime attack. Many intrusion detection devices, such as closed circuit television (CCTV) systems, require proper lighting to be effective. Guards and sentries need proper lighting in order to correctly perform their duties.

The Military Handbook of Design Guidelines for Physical Security of Fixed Land-Based Facilities (DM-13.1), lists several lighting specifications for different areas. The specifications list required foot candles at ground level for areas such as entrances (2.00 or 1.00 foot candles) and isolated fenced boundaries (0.15 foot candles). The specifications also list the width of lighted boundary for each type of area. For example, isolated fence boundaries should be lit for an area of 10 feet inside and 25-200 feet outside.[21]

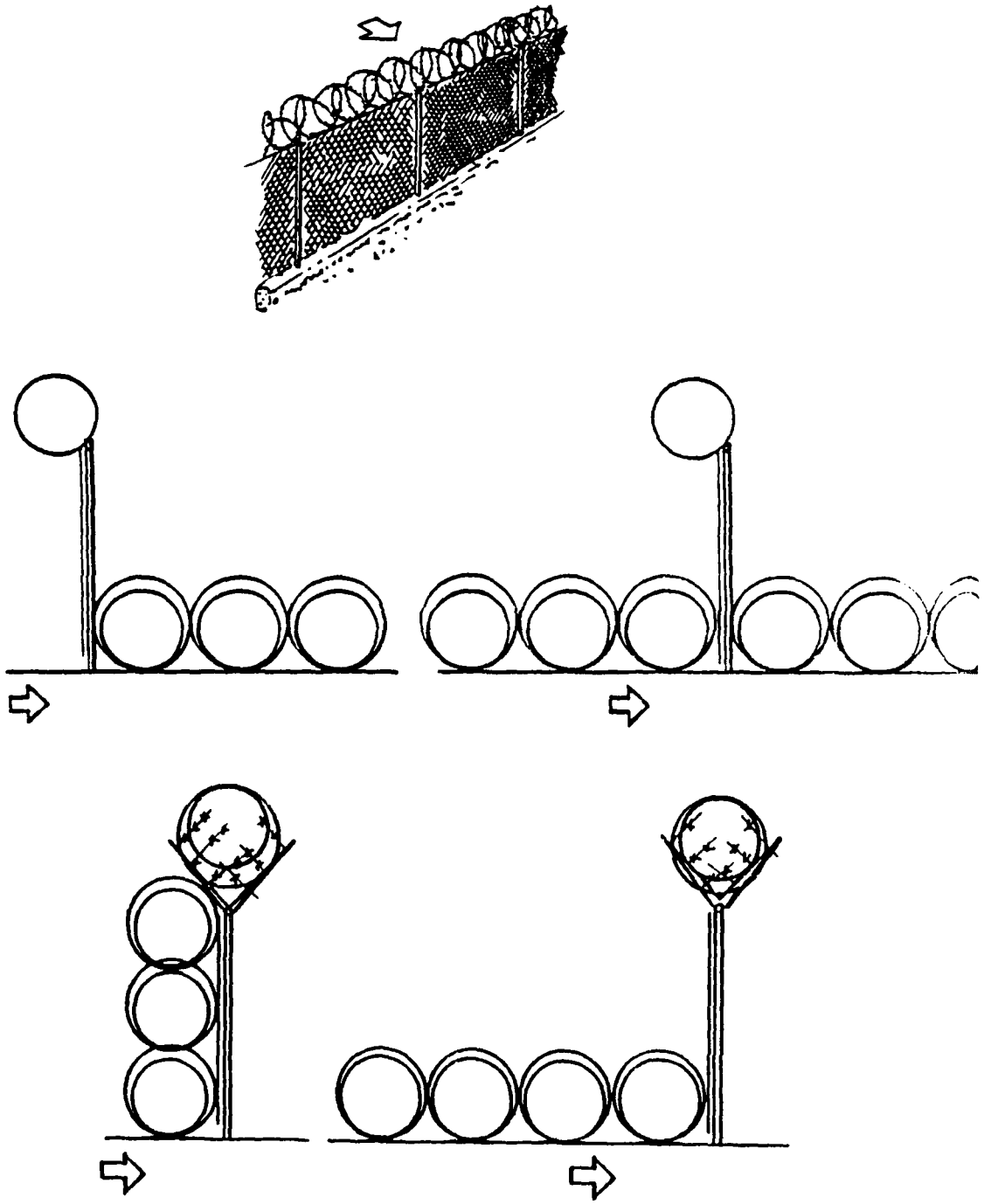


Figure 3.2: Fencing Options
(from *Design Guidelines for Physical Security of Fixed Land-Based Facilities, pp. 135*)

Lighting can be provided by fixed light fixtures or movable fixtures (light trucks). The type of light used should be based on the amount of light needed, maintenance costs and operating (energy) costs. Lighting should be placed in areas where it is most needed to reduce the probability of attack from a relatively unprotected area or to eliminate shadows where lone terrorists or small group may hide.

It should be noted that tests have shown that lighting provides a deterrent only to the unsophisticated and undedicated intruder. Thus, lighting will not usually deter a terrorist. Also, before significant funds are spent on lighting, a study may be made on whether an attack at night is likely. The threat analysis should answer that question. Although the terrorist will normally strike during the day in order to get the maximum shock value, it is very possible that a terrorist bomb may be planted at night.

3.2 Intrusion Detection Systems

Another method of countering a terrorist attack is through the use of an integrated intrusion detection system (IDS). Intrusion detection systems allow detection of an intruder, such as a terrorist, early in his attack. The objective of the IDS should be to detect the intruder early enough for the security force to take effective preemptive action. For this reason,

the IDS must start with the perimeter, or even outside the perimeter.

There are many types of intrusion detection systems. Which type should be installed will depend on factors such as the type of threat, layout of the facility, what needs to be protected and how much the owner can afford. IDS should be designed as a part of the total facility security system.

One of the simpler types of IDS is the **taut-wire detector.** The taut wire detector is basically a trip wire connected to an alarm. Taut-wire detectors can be run along various points in a fence and can detect an intruder that may be attempting to climb over or under the fence or that may try to cut through the fence. They can also be used as trip-wires either just inside or just outside the fence.

Other sensors used in a similar manner as the taut-wire are the **tilt and vibration switch detectors.** These are switches that are set to close, and thus set off an alarm, whenever they are tilted or vibrated. These switches can detect movement along a fence or by a doorway.[22,23]

Other electromechanical systems include **metallic foil** that is used on windows. This metallic foil has a current running through it that will set off an alarm when the circuit is broken by an intruder breaking the

window. **Magnetic contact devices** are used on doors, windows and gates. These devices set off an alarm when the contact is broken by opening the door or window. **Window lacing**, or wooden screens with fine wires running through the slats, can be made to look like normal window shutters but will set off an alarm if the wires are broken during an entry attempt.

Electromechanical devices have several disadvantages, most important being their ease of detection by an experienced intruder. More sophisticated devices, including microwave, electric or magnetic fields, infrared and CCTV, have become increasingly popular.

In **microwave sensors**, microwave energy is continuously beamed from transmitter to receiver. An alarm goes off whenever the field is broken or deflected. **Infrared beam sensors** work in a similar manner using an infrared light beam.

Electric field and **electric capacitance sensors** measure changes in electric fields or electrical capacitance and will sound an alarm when the measurements change a specified amount. These sensors are normally used to detect intruders who may be attempting to climb over barriers or fences.

Some buried-line sensors have been proven effective. These include **pressure sensitive buried-line** and **magnetic buried-line** sensors. The pressure sensitive

lines are normally oil filled hoses with pressure sensitive switches at the ends of the lines. Movement over the lines causes pressure changes in the hoses. A related device is the **seismic buried-line** sensor, which uses geophones to detect seismic vibrations from intruders walking over them. The magnetic buried-line sensors can detect changes in the magnetic field as an intruder passes over them. This is sensitive to ferromagnetic material and therefore is useful for detecting individuals that may be carrying weapons.

Video motion detectors are used in conjunction with CCTV systems. These detectors sound an alarm when the electrons moving into the field of view are excited due to movement detected by the CCTV camera.[24]

Other intrusion detection systems are availabe on the market. These include pressure sensitive mats, audio detection systems, photoelectric devices and vibration detectors.

All of the above detectors have their advantages and disadvantages. Some are susceptible to false alarms from such things as large animals, lightning and wind or their effectiveness may be reduced by weather conditions such as fog (in the case of infrared and photoelectric devices). However, in a high threat facility, especially one which may be subject to terrorism, no one intrusion detection system should be relied upon.

Rather, a defense-in-depth concept should be employed where several IDS systems are employed in succession. This can reduce false alarms along with increasing the detection probability. A terrorist may neutralize one system and still be detected by another. By using IDS in conjuction with barriers, access control, facility hardening, etc, a true layered defense can be achieved.[23]

3.3 Vehicle Barriers

The car bomb: fast, effective, deadly. In 1983, it was a car bomb that drove through the perimeter of the U.S. Marine barracks, exploded with over 12,000 pounds of TNT and killed 241 U.S. military personnel. From January 1980 to March 1986, there were 13 car bomb attacks against overseas U.S. Government facilities.[24] The car bomb is one of the most popular terrorist weapons in use today. The need to design effective means of stopping this threat is evident.

3.3.1 General Considerations

The primary objective of a vehicle barrier is to stop a vehicle from entering the compound. Some barriers may be meant to only slow a vehicle down, allowing sufficient reaction time to minimize injury and damage. There are many considerations a designer must take into account when deciding whether or not to install a vehicle barrier system and, if so, what type

should be installed.

First, as in the design of any security system, the threat must be determined. The type of vehicle bomb and probability of attack should be estimated. The size and speed of the vehicle should also be estimated. The possible locations of entry of car bombs should be determined and the criticality and vulnerability of each entry point should be examined.

The probable size and speed of the car bomb is one of the most important factors in designing the proper vehicle barrier. A common method of evaluating the performance of vehicle barriers is in terms of the penetration it allows of certain weight vehicles with specific speeds. The Department of State lists the following penetration standards for vehicle barriers:[27]

Performance Level	Crash Test Criteria
L3.Ø	Vehicle is stopped with partial penetration or barrier deflection of three feet.
L2.Ø	Vehicle is stopped with maximum penetration of twenty feet.
L1.Ø	Vehicle is disabled and does not travel more than fifty feet after impact.

Table 3-1 shows the U.S. Navy standards for vehicle barriers.[28]

Table 3.1

Parameter	Requirement
Net explosive weight	1,000 pounds
Gross vehicle weight and speed	(1) Where barrier is near property boundary or speed cannot be restricted: 10,000 pound vehicle at 50 miles per hour (0-10 foot penetration) or (2) Where barrier is located an adequate distance from building and speed can be restricted: 10,000 pound vehicle at 15 miles per hour (50-100 feet penetration)
Life expectancy	5-10 years
Operating time	0-3 seconds
Operating temperature	-65 to 120 (°F)
Mean time between preventive maintenance	1 month
Mean time for preventive maintenance	2 man-hours
Mean time between repairs	1 year
Mean time for repairs	1 day

Vehicle speed can be estimated using figure 3-3 for a passenger car or 2.5 ton truck. This figure is based on an assumed acceleration from a standing start of 11.27 feet per second for the passenger car and 5.80 feet per second for the truck. The following formula can be used to estimate the speed for other conditions if the acceleration is known:

$$V(mph) = 0.68\ (2sa)^{0.5}$$

Where: s = distance (feet)
a = acceleration (ft/sec^2)

Curves in a road leading to a vehicle barrier can also slow a vehicle down. Figure 3-3 shows at what speeds a vehicle will normally start to skid based on the turning radius of the curve. This curve is based on the following formula:

$$R = V^2/14.96$$

Where: R = curve radius (ft)
V = speed (mph)

It is therefore evident that the size and speed of the vehicle should be estimated accurately. Also, roads leading into the protected area should be curved whenever possible. Any other method that may be used to slow vehicles down prior to reaching the gate will also allow the use of less stringent vehicle barrier design.

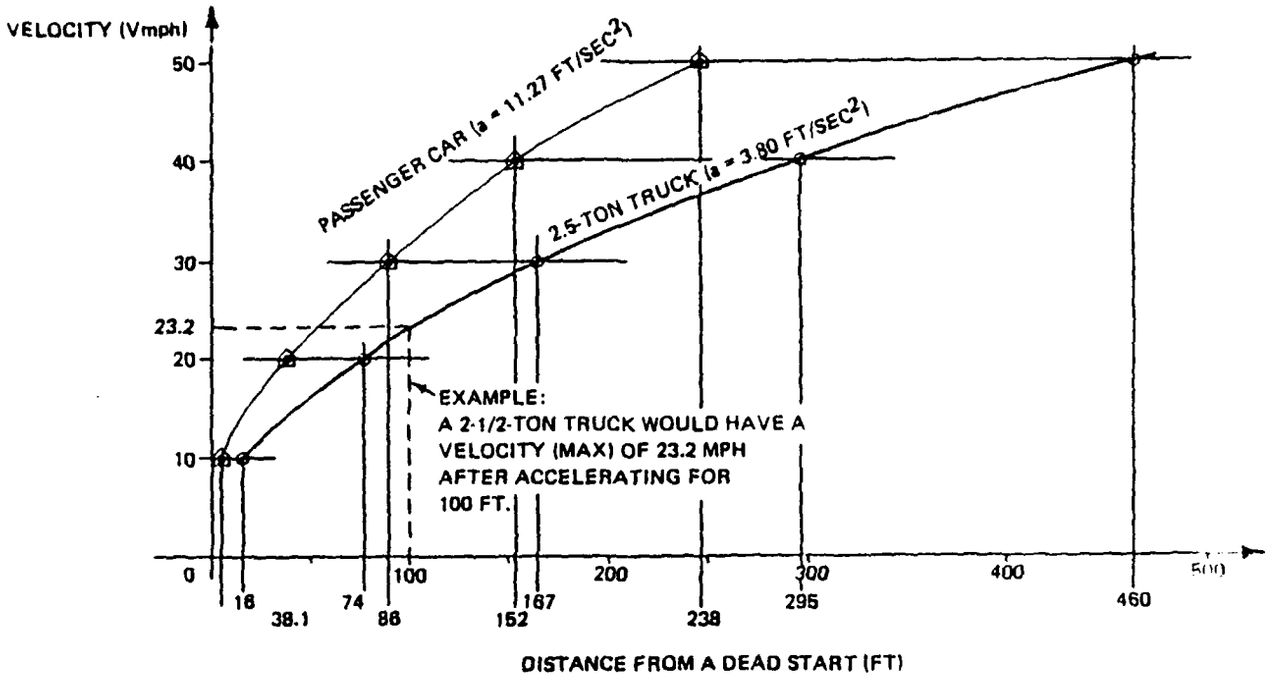


Figure 3.3: Vehicle Velocity
(Terrorist Vehicle Bomb Survivability Manual, p.3-8)

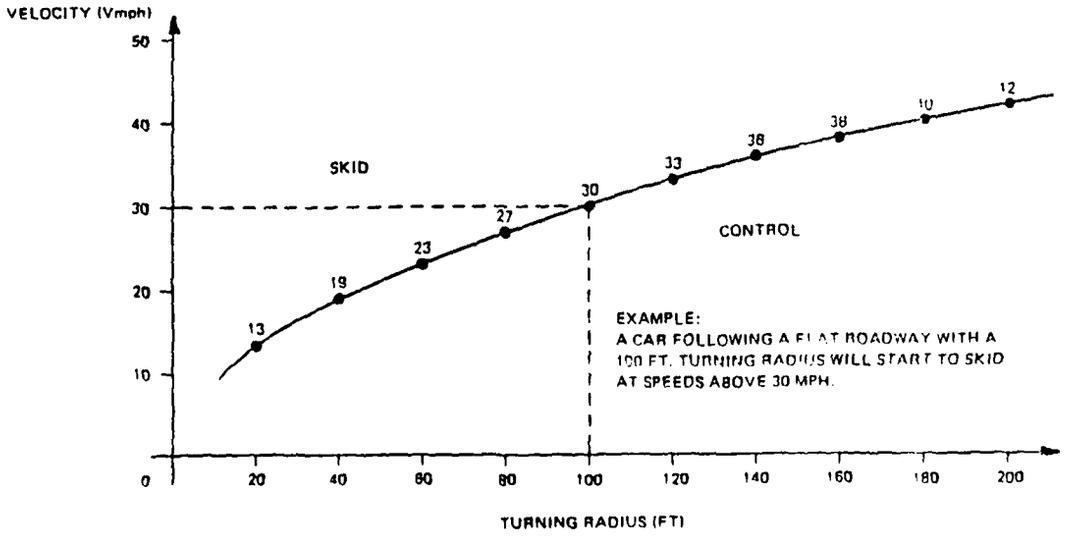


Figure 3.4: Turning Radius
(Terrorist Vehicle Bomb Survivability Manual, 3-10)

Other factors that will influence vehicle barrier design include aesthetics, the space available, whether or not a guard or sentry is stationed at the gate, reliability, maintainability and safety. Vehicle barriers are on the market that are hidden from view until activated, which is good from an aesthetics viewpoint, but they also require someone to operate them. Using planters as vehicle barriers can provide cover for terrorists. A disasterous example of this occurred when the American embassey in Saigon was attacked in January 1968. Viet Cong terrorists had managed to blast their way into the embassy compound and held onto the grounds, though not the embassy itself, by using concrete planter boxes as cover from which they could fire.[29]

Vehicle barriers should be located at probable attack sites. Another factor to consider in deciding their location, however, is the proximity of the building to be protected. Sufficient separation distance should be designed so as to minimize damage from the shock of a car bomb explosion upon contact with the barrier. Using the Navy criteria of 1000 pounds of explosive, structures within a 400 foot radius could receive light to heavy damage from the blast. If sufficient clear distance cannot be provided, the

facility may have to be hardened or blast walls installed.

Often, kinetic energy is used to compare the effectiveness of vehicle barriers. Kinetic energy can be expressed by the following formula for vehicle crash threats:

$$KE = 33.44 \times 10^{-3}(wv^2)$$

Where: KE = kinetic energy (foot-pounds)
w = vehicle weight (pounds)
v = vehicle speed (mph)

Therefore, if a vehicle weighs 10,000 and impacts the barrier at 40mph, the resultant kinetic energy is 535,040 foot-pounds. Any barrier that can withstand that force is adequate for the threat.[31]

The entrance to a protected facility could be divided into three zones for design. The first zone would be the approach and would consist of designs used to slow vehicles down, such as curves and speed bumps. The approach zone would vary in length and would connect the checkpoint (guardhouse or gate) with the public road. The second zone, the blast zone, is at least 400 feet long and is between the guardhouse and the barrier. This zone provides safety for the sentries and time for an active barrier system to be activated. The third zone, the safety zone, provides space between the structure to be protected and the barrier. It should be at least 900 feet for an explosion of 10,000 pounds TNT.

Blast barriers may be installed in this zone if adequate distance is not available.[22]

3.3.2 Vehicle Barrier Types

There are two categories of vehicle barriers, passive and active. Passive barriers do not need to be activated in any way. Active barriers require action by personnel or equipment to deploy and thus selectively permit entry. Active barriers normally require a power source to operate and are activated automatically by trips or sensors or manually by sentries or security personnel using remote switches. A brief discussion of several types of passive and active systems follows:

3.3.2.1 Passive Vehicle Barriers

Passive barriers are simple and inexpensive, but they are limited in their use and effectiveness. Passive barriers can be fixed structures, such as walls, bollards, ditches, lakes or streams, guardrails and others. They can also be movable, such as logs, boulders, curbs or highway medians. Each has advantages and disadvantages. Some of the more popular passive systems are described below:

Concrete barriers, especially the New Jersey highway median barrier, are normally inexpensive and may be fixed or relatively mobile (they can be placed in position within a small amount of time if the proper

equipment is available). They are relatively effective at small impact angles (less than 30 degrees). Full penetration can be achieved, however, by a light vehicle, but not without damage. Tests resulted in a 4000 pound vehicle at 50 mph penetrating 20 feet with extensive damage to the vehicle and probable serious injuries to the occupants. A summary of test results of many barriers, as conducted by the Naval Civil Engineering Laboratory, are given in Appendix A.

Concrete bollards are a fixed system of 8 inch diameter steel pipe (1/2 inch thick) filled with concrete. They normally extend 3 feet above ground and have a 4 foot deep footing. This system is effective as a backup system to a fence to stop vehicles that may attempt to crash through the fence. They can also be used to direct traffic and prevent vehicles from crossing fields to reach sensitive structures, thus bypassing the main roads.

Concrete planters can be used as vehicle barriers and they are aethsetically pleasing. Their effectiveness as vehicle barriers is good (a 15,000 pound vehicle at 47 mph penetrated 31.2 feet). However, as already mentioned, care must be taken not to provide an attacker the cover that a planter might provide.

Fences can be used as vehicle barriers if they are reinforced sufficiently with concrete and cables.

However, even reinforced, they are not normally considered adequate to function as vehicle barriers alone. Cable reinforced fencing has proven capable of stopping vehicles (see Appendix A).

Ditches and **earth barriers** can be very effective vehicle barriers to use around the perimeter of a facility. **Sand filled drums, curbs, logs** and similar barriers are used most often to direct traffic or to slow a vehicle down. Sand filled 55 gallon drums can effectively stop a vehicle if enough of them are used to absorb the vehicle's kinetic energy.

It should be noted that concrete and masonry walls are generally not considered useful as vehicle barriers. Tests on these walls have shown that full penetration was achieved.

There are many other type of passive barriers available. Some are available on the commercial market, others, such as ditches and logs, can normally be constructed using local equipment and material. Even heavy equipment tires half buried in the ground can stop light vehicles. When considering passive vehicle barriers, aesthetics, cost and effectiveness must be taken into account.[33]

3.3.2.2 Active Vehicle Barriers

Passive vehicle barrier systems have several

disadvantages. The time involved in getting some of them into position is one. They cannot be used to block a road as that would also prevent authorized vehicles from passing through. In order to allow for selective vehicle access, many different types of active systems are available.

When selecting active systems, the means for activating the system is important. The active systems can generally be activated by buttons or switches from the guardhouse but they can also be set to operate automatically if necessary. Some systems, such as mines in the roadway, can be command controlled. All systems should have a back-up means of control. Guards in a guardhouse should be able to activate the system even if wounded. If an automatic system fails, there should be a method of activating it remotely.

There are many types of active barriers. A few of the more common barriers are described below:

The **Babcock and Wilcox Arrestor** (see figure 3.5) is a system that uses pointed steel beams that are operated pneumatically to stop a vehicle. It has been found to be very effective. When lowered, the system is flush with the roadway and vehicles can pass over it. When raised, the system will stop most vehicles with little to no penetration.

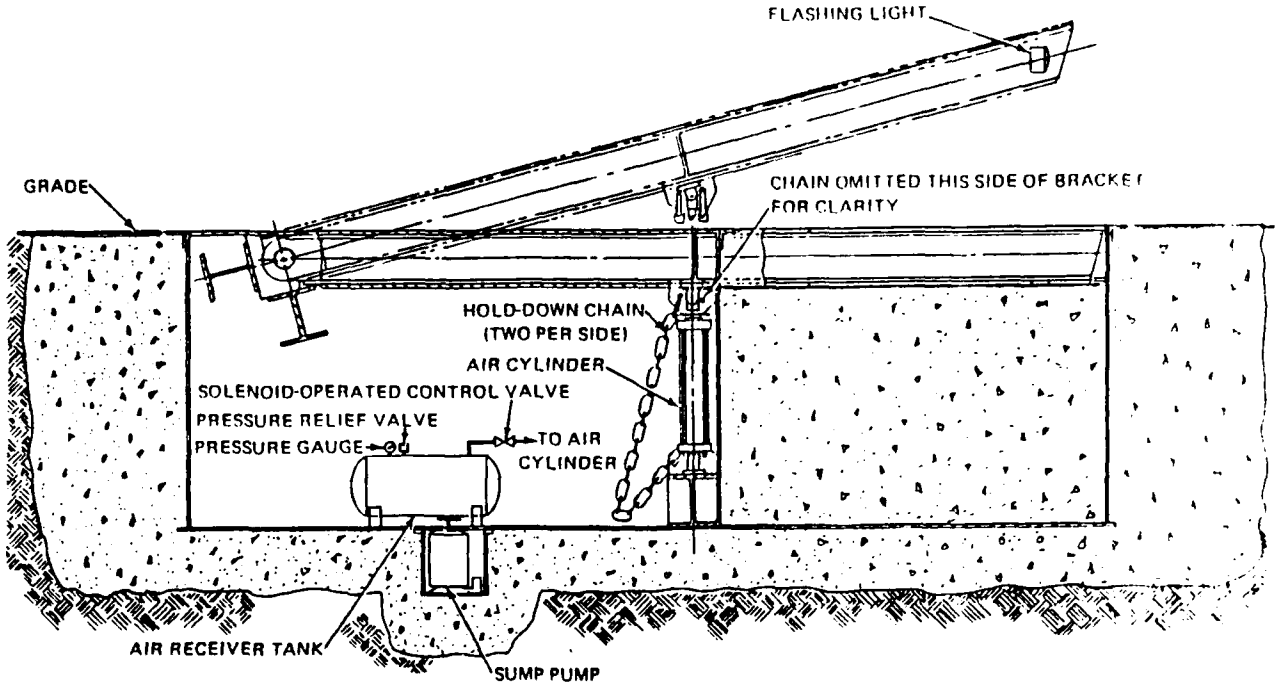


Figure 3.5: Babcock and Wilcox Arrestor
(from *Terrorist Vehicle Survivability Manual, March 1986*, p.7-2)

Barricade systems are normally hydraulically operated units that use steel or concrete barricades to stop the vehicle. These units can come in a variety of sizes and shapes. For example, the **Delta TT2078 Phalanx** (figure 3.6) system rises to a height of 38 inches. A test vehicle of 14,815 pounds at 49.9 mph penetrated 3.4 feet but was also totally destroyed.

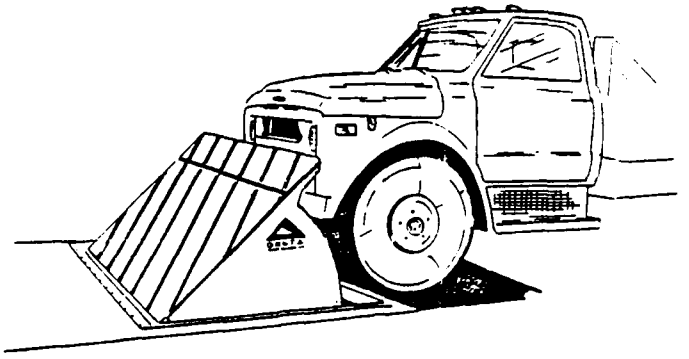


Figure 3.6: Delta TT207S Phalanx Vehicle Barrier
(from *Terrorist Vehicle Bomb Survivability Manual March 1986*, p. 7-8)

The **Delta TT120 Hydraulic Bollard System** consists of a 10 inch diameter steel bollard that is vertically raised into position. A 15,180 pound vehicle at 30 mph penetrated the barrier 2.4 feet.

The Entwistle Dragnet system uses a chain link net attached to metal tape that is drawn through energy absorbers to stop vehicles. The energy absorbing device acts as a brake that slows down and eventual stops the vehicle. The net system is held in an elevated position, allowing authorized vehicles to pass underneath, until deployed. To stop heavy, fast moving vehicles, a second net located at some distance beyond the first may be needed. The single net system allows

penetrations of up to 50 feet.

The **Western Portapungi** (see figure 3.7) is a barrier designed to immobilize a vehicle by engaging the front axle. It is very mobile, installation time being only minutes, and therefore can be moved from point to point.

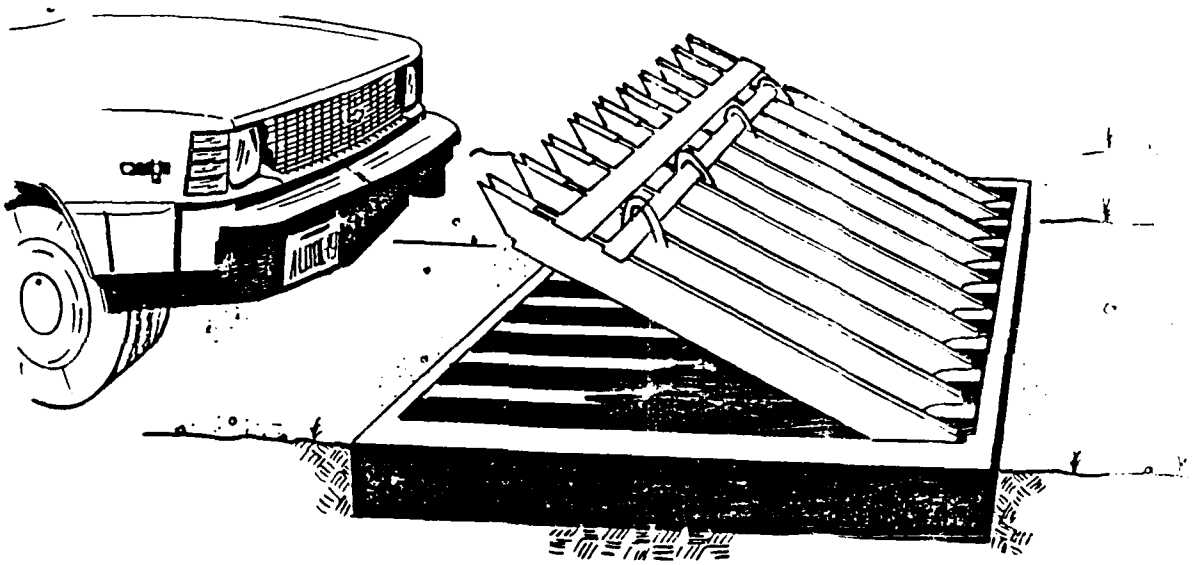


Figure 3.7: Western Portapungi Vehicle Barrier System
(from *Design Guidelines for Physical Security of Fixed Land-Based Facilities*, p. 224)

There are many other types of active barrier systems and new types are being tested. Anti-driver devices include bright lights set to shine in the driver's eyes, anti-personnel chemical agent dispensers and visibility reducing fog dispensers. Active barriers that force vehicles off the road into a swamp, ditch or other hazard are also possibilities. Using reverse banked

curves with friction reducing agent dispensers is another possibility. Pits that are normally covered by a ramp, which drops upon activation, are another type of active barrier system. It should be noted that tire shredders are popular vehicle barriers but their effectiveness is limited. A determined terrorist will drive right through tire shredders and just keep on going to his objective. Also, barriers that threaten the occupants with death but do not stop the vehicle may be ineffective against suicide bombers.

Although active barriers allow selective access to an installation, they are often more expensive than passive barriers. Active barriers also require more maintenance than passive barriers. One other factor to keep in mind when selecting an active barrier is its cycle time, how soon after deployment can it be lowered and how fast will it deploy when activated. These can be critical factors in determining type and location of the barriers. Most cycle times can be obtained from the manufacturer or from tests made by other organizations, such as NCEL.[34]

Other considerations include avoiding installing underground active barriers if the installation cannot be drained properly or if the ground is subject to severe soil conditions such as freeze/thaw effects. An alternate traffic route should be available but should

not be usable unless needed. Active barriers normally rely on power sources. These sources should be protected and an emergency source of power should be available to the vehicle barriers. The exits as well as the entrances should be protected. Figure 3.8 shows the general effectiveness of several types of vehicle barriers. Appendix A lists penetration test results for many common vehicle barriers.

3.3.3 Vehicle Barrier Design

Figure 3.9 is a decision tree that will aid the security engineer in the design of a vehicle barrier system. Similar decision trees can be developed for other components of security design.

3.4 Tunneling

In some instances, a sophisticated attacker may gain access to a facility through tunneling. If the tunneling threat is significant, the security engineer must design measures into the facility that will reduce the threat. There are several means that can be taken to defend against a tunneler. Reinforcing the floor slabs will deny the intruder access to the building by coming up through a tunnel. However, a terrorist may still tunnel to the floor in order to plant a bomb under the facility.

To guard against any tunneling intrusion, motion detectors such as seismic detectors, electrical

capacitance detectors and others can be used to detect tunneling activity. Underground barriers such as sheet metal or buried fence fabric can be used to impede tunneling if the threat warrants. Natural terrain characteristics, including ditches, streams and trees with deep root systems, can also inhibit tunneling. Perhaps the best defense against a tunneler, however, is for the guards to keep their ears and eyes open in and around the facility.

ACTIVE BARRIERS:

High:

- -Barricade Ramp
- -Hydraulic or Motorized Barrier
- -Pit Barrier

Medium:

- -Cable-Reinforced Gates/Fences
- -Crash Beams
- -Sliding Lift/Swing Gates
- -Steel Cable Barriers

PASSIVE BARRIERS:

High:

- -Angled Posts
- -Bollards
- -Concrete Barriers
- -Earth-filled Barrier
- -Excavations/Ditches
- -Heavy-Equipment Tires

Medium:

- -Enhanced Fences
- -55-Gallon Drums
- -Guard Posts
- -Sandbags

Low:

- -Barbed Wire Fence
- -Metal guardrails

Figure 3.8:Barrier Effectiveness Chart
(Terrorist Vehicle Bomb Survivability Manual, March 1986, pg 3-5)

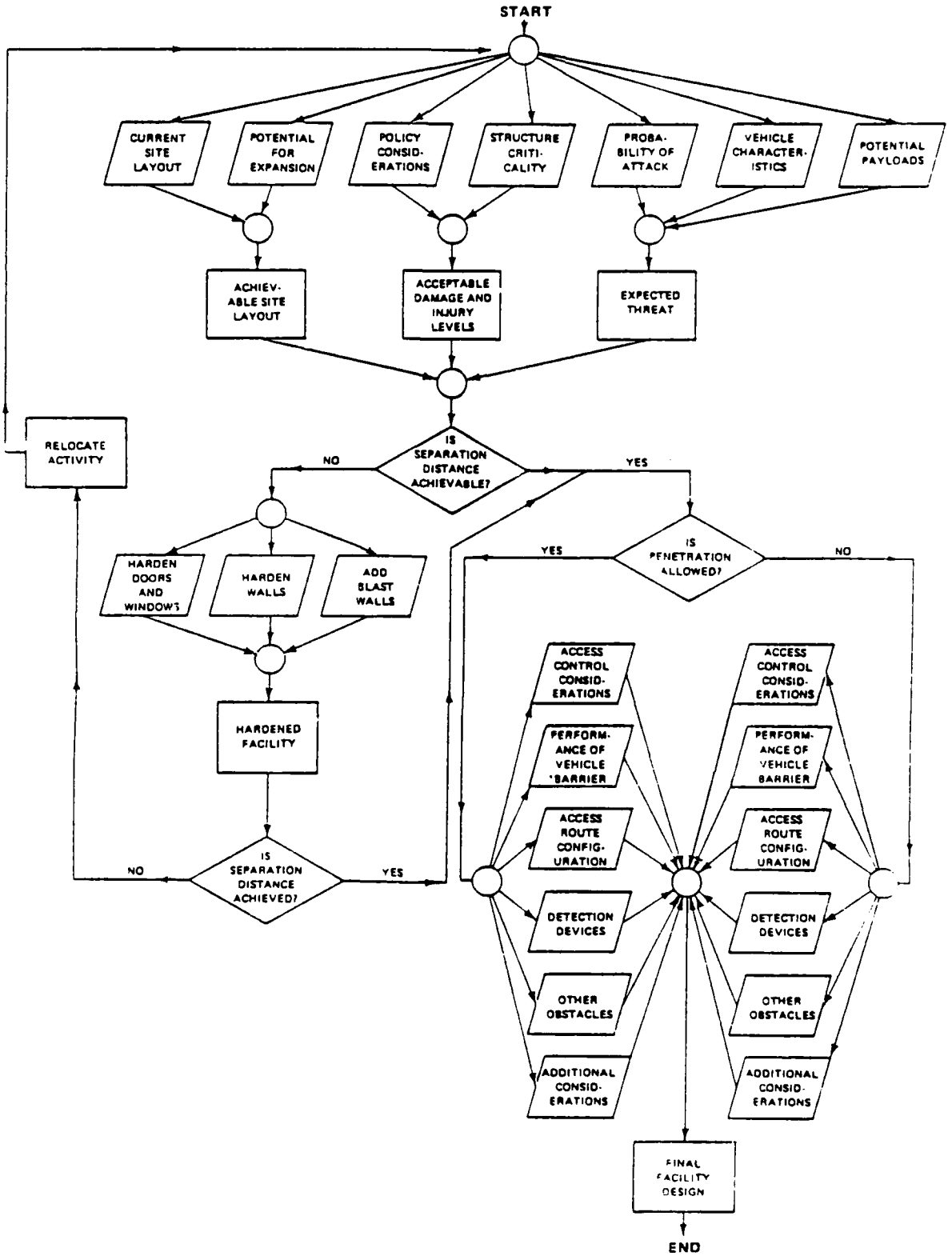


Figure 3.9: Vehicle Barrier Decision Tree
(from *Terrorist Vehicle Bomb Survivability Manual, March 1986*, p. G-3)

CHAPTER IV

STRUCTURAL SECURITY

4.1 General Considerations

Defense of the perimeter is important. However, even a well designed perimeter defense is not fool-proof. A sophisticated and dedicated terrorist with modern weapons will probably find a way through a perimeter defense. The next question the security engineer must address in his design is to what degree the structure itself must be hardened and what methods of facility hardening should be used. Again, there are many factors that must be taken into account.

As in the design of the perimeter, the threat is one of the most important factors to be considered when designing the building to be protected. If the threat is an organized group of terrorists with access to explosive weapons, the facility will have to be designed to withstand direct hits by rockets or explosives. If the threat is a lone intruder, then protection from small arms and intrusion may be all that is necessary. Whatever the expected threat, the facility should be built to survive an attack.

Another consideration is whether or not any loss is acceptable. The cost to fortify a building against direct rocket attack, for example, may be prohibitive.

Therefore, the owner and designer may decide that the loss of parts of the building is acceptable and therefore only certain sections of the facility may be hardened against attack. An interior vault or specific interior rooms may be heavily protected while the exterior portions of the structure are constructed of standard building materials. Only protecting what needs to be protected can save funds that may otherwise be spent unnecessarily. Cost versus loss is an important design parameter for the security engineer.

In deciding the degree of hardening necessary to adequately protect the structure, the perimeter defense should be taken into account. A strong perimeter defense along with sufficient clear zones and safety zones may reduce the amount of facility hardening required. For example, if the vehicle barriers must be located too close to the structure, even if the vehicle is stopped, shock waves from the ensuing explosion could severely damage a structure. In that case, the structure would have to be protected by additional hardening or by such things as blast walls. Appendix B contains examples of the pressures that structures should be designed to resist for specific explosive charge weights.

4.2 Construction Options

When designing a facility to resist a terrorist attack, several options are available to the engineer. The two most important aspects are the choice of materials used and the dimensions of walls, roofs and floors, as well as the building geometry. In general, the normal design procedures used to design structures should be followed by the security engineer only with the additional forces that may be added due to a direct hit or to a proximity explosion. These additional forces can be calculated once the probable threat is known.

4.2.1 Wall and Roof Construction

In the design of walls and roofs that may be subject to ballistic or explosive attack, reinforced concrete has proven to be the only effective conventional material for attack-hardened facilities. The hardening options for reinforced concrete walls and roofs (and floors of multi-story buildings), include increasing the thickness of the wall, increasing the reinforcing steel (increasing the reinforcement bar size or number of layers), or decreasing the reinforcement bar spacing.

Another hardening option for reinforced concrete is to use steel-fiber-reinforced concrete. The fibrous concrete adds significantly to the penetration time of a

wall against an intruder trying to gain entrance through the wall. However, reinforced fibrous concrete is also more expensive than conventional concrete.

There are many more options for the construction of walls, including masonry walls (concrete masonry units), and stud/grit walls. However, even with reinforcing options available to these walls, they are generally inadequate for protection against terrorist attack. One other hardening option is to use composite materials. A layered system of steel/polycarbonate panels offer penetration resistance and are usefull for retrofitting existing structures.

4.2.2 Blast Barriers

Current technology for protecting buildings from blast loading involves heavy reinforcement of exterior concrete walls as described above. These walls are normally cast integrally with heavily reinforced floors and columns. Windows must be thick and small in order to resist the blast loads. This type of design can be expensive to construct, especially in areas where materials and skilled labor may not be readily available. The walls and components such as windows and doors may be subject to local failure which could allow deadly shrapnel to enter the building even if the wall itself was strong enough to resist the blast. These walls are expensive to repair if damaged by a blast.

Designing buildings using heavy reinforcement often results in a fortress-like appearance.

The many disadvantages of current reinforced concrete design for protection against blast loads have led to newer technologies that eliminate some of the disadvantages. One of these new methods that is currently being developed is the "blast barrier."

The blast barrier is a wall section that relies on friction to absorb the energy of a blast wave. Wall panels are constructed of conventional materials such as precast concrete or masonry block. The wall panels are mounted on tracks that extend about two feet into the building. When hit with a blast load, the wall panel will slide along the tracks dissipating the blast energy and avoiding collapse. Since the wall does not have to be built to withstand the full blast load, it is less costly than the standard monolithic walls and columns. The blast barrier has an approximate cost savings of 13% over the conventional construction system. The savings is due to less materials, concrete and reinforcing steel, required and simplified construction.[35]

The blast barrier system is based on the conversion of the blast impulse energy into kinetic energy of the wall. This kinetic energy is then dissipated through friction brake shoes as the wall slides into the building along its shallow tracks. The wall will only

move when the minimum blast barrier pressure is exceeded by a blast loading. The minimum blast barrier pressure can be calculated as follows:

$$Pbb = \mu N/A$$

Where: Pbb = minimum blast barrier pressure;
μ = coefficient of friction;
N = the total in-track prestress force;
A = area of wall exposed to blast.

The total in-track prestress force is adjustable, thus the minimum blast barrier pressure is also adjustable. The displacement of the wall subject to certain blast pressures above the minimum blast pressure can be controlled by proper design of the weight of the wall, the prestress force or the coeficient of friction.

Figure 4.1 shows a typical detail of a blast barrier window wall. The tracks are embedded in the sides of columns, floors and ceilings formed with a reusable rigid template. A steel bar in the tracks is used to align the precast walls accurately. The steel bars fit through teflon sleeves in the wall panels. The slide plates can then be prestressed using a load cell to compress the wall against each track. This determines the prestressed force, N, which then determines the reaction force necessary to cause movement of the wall as described above (see figure 4.2).

The minimum blast barrier pressure should be designed to be well below the strength of the wall itself. Any blast pressure exceeding the minimum pressure will then cause the wall to accelerate into the building, dissipating the blast pressure until stopping several inches inside the building. Thus the wall panel itself is not damaged. To repair the wall after the blast, it is simply necessary to jack it back into position and prestressing it again into the tracks.

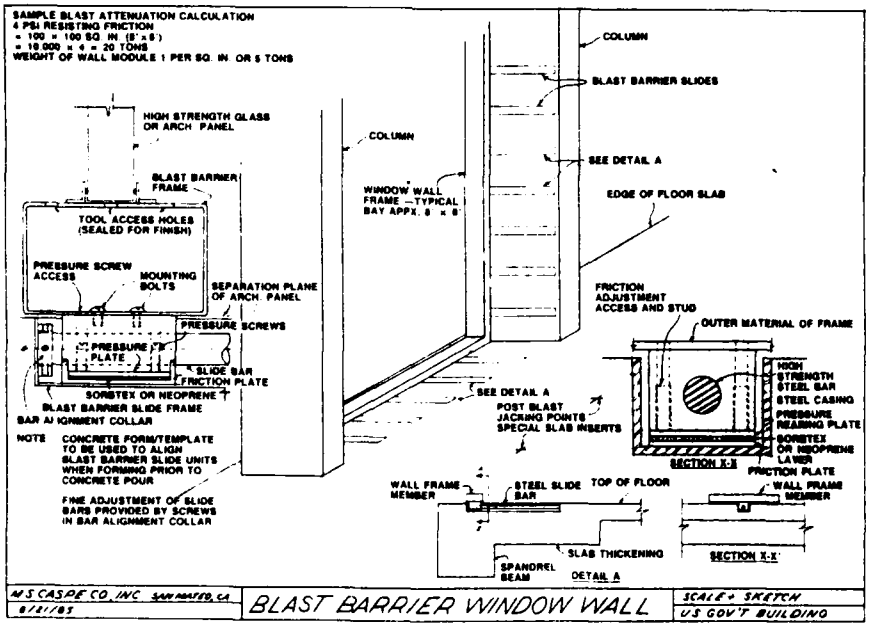


Figure 4.1: Typical Detail for a Blast Barrier Wall
(from M.S. Caspe, "The Blast Barrier," p. 100)

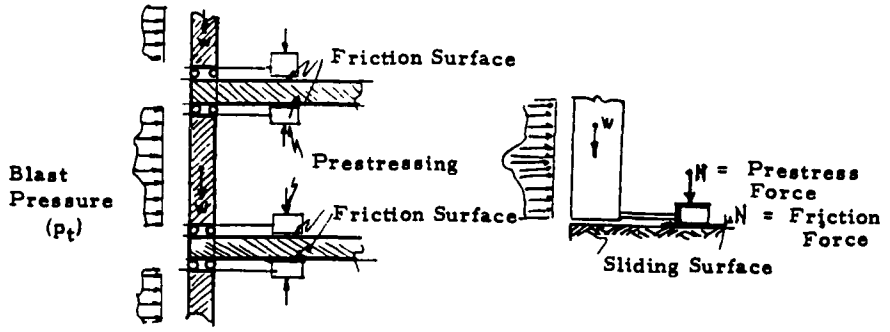


Figure 4.2: Mathematical Model of Blast Barrier
(from M.S. Caspe, "The Blast Barrier," p. 101)

The blast barrier offers not only cost advantages, but it also offers more architectural freedom by allowing the use of any locally available materials. The windows, door and wall have to be designed only to meet the reaction force, with an appropriate factor of safety, and not the full force of the blast. Thus the windows can be designed to be larger and thinner. The lower the strength of the wall materials, however, the further the wall will have to travel into the building. The blast barrier can be very useful if space limitations prohibit proper clear zones between a building and its perimeter defenses.

Since the blast pressure is not necessarily uniform, a safety factor should be used to prevent local spalling of the concrete which could result in shrapnel being expelled into the building. This will result in

slightly more reinforcement than would otherwise have been necessary. The blast barrier may also be used to retrofit existing buildings by adding a facade 5 to 20 feet from the existing exterior wall. This could add more floor space to the building.

The blast barrier can also be designed as a perimeter wall system. In this capacity, the blast barrier will absorb the impact of a vehicle and the blast of a vehicle bomb. Properly designed, the blast barrier will eliminate problems associated with conventional concrete perimeter walls, including shrapnel hazards and the probability of the vehicle rolling over the barrier and exploding on the inside of the perimeter.

The perimeter blast barrier system is constructed by bolting portable 8x8x32 inch long steel boxes together with horizontal and vertical bolts that can be pretensioned to control frictional slippage between boxes. The boxes may be filled with sand and reinforced with a cable (see figure 4.3). The pretensioned forces determine at what force the boxes will begin to slide against one another and the friction between boxes plus additional viscous damping provided by the cable will dissipate the energy of the vehicle and lesson the effects of the blast pressure. The perimeter wall will distort vice rupture. The wall could be covered with an

architectural treatment. The components are easy to transport and erect. Repair of the wall simply involves replacing boxes that are severely damaged and re-erecting those that are not badly distorted.[34]

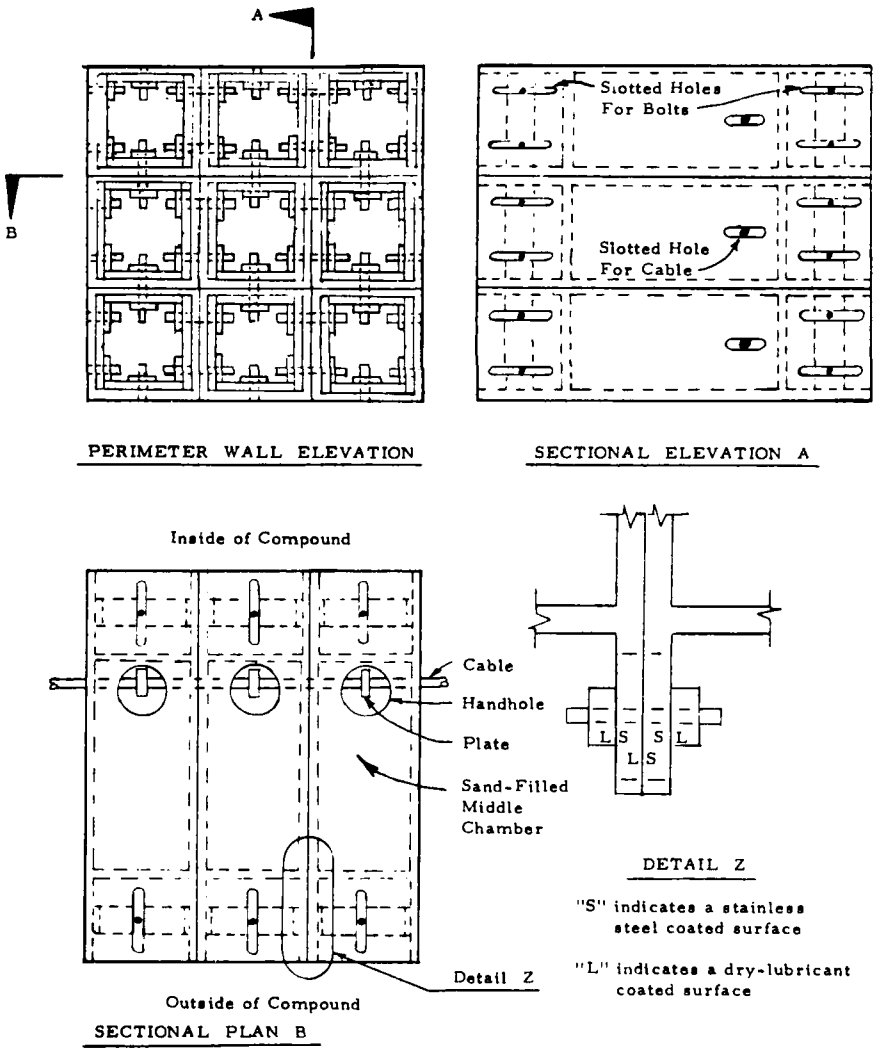


Figure 4.3: Perimeter Blast Barrier System
(from M.S. Caspe, "The Blast Barrier", p. 102)

The blast barrier system is a viable alternative to conventional reinforced concrete that can result in significant cost savings without sacrificing any protection. As technology and research continues, more efficient building systems that are blast resistant will be developed. For example, a system similar to blast barriers is being studied for protection of roofs. This system would provide a sacrificial roof over the permanent structure. The sacrificial roof would be designed to detonate and attenuate bomb blasts.

4.2.3 Window Treatment

Many of the injuries resulting from terrorist bombings and accidental explosions are caused by the fragments of blasted-out window glazing. If windows are not adequately protected against blast loadings, they can also subject the occupants to blast pressures, secondary debris and other blast effects. Providing blast resistant windows in high risk facilities is a necessity in order to adequately protect the occupants.

Acceptable materials for resistance to blast overpressures include monolithic thermally tempered glass, laminated thermally termpered glass and laminated Herculite II (chemically tempered glass). Unacceptable materials for blast resistance include chemically tempered glass (other than Herculite II), annealed

glass, heat-treated semitempered glass, wire-reinforced glass and acrylic (Plexiglass or Lucite). Polycarbonate materials are still being tested.[37]

The acceptable materials should be used for design of structures that are to be blast resistant. The Naval Civil Engineering Laboratory has developed design procedures for determing the required thickness of the glazing based on threat (charge weight) and aspect ratio (ratio of long side to short side of the window). The tables used for this design procedure are published in the March 1986 edition of *Terrorist Vehicle Bomb Survivability Manual* and the *Design Guidelines for Physical Security of Fixed Land-Based Facilities.*

If bomb fragments are a concern in the design of particular windows, a polycarbonate fragment retention film should be applied to the inside of the window to hold the glass in place. These films are available commercially. The recommended thickness of the film is 1/2 inch. This film has been found to be effective in short duration, small, close-in explosions but not as effective in longer duration explosions.[38]

The windows need not be designed to be any stronger than the surrounding wall and frame. Frame design is another important consideration for designing windows.

Window frame loading as transmitted by the blast and window glazing is shown in figure 4.4. The line loads

and corner loads have been reduced to a static structural design problem with the coefficients of C_x, C_y, C_r and the structural equivalent design load, r_u. These coefficients are tabulated in the two publications previously mentioned.

The maximum stress limitations for metal frame members are as follows:

- $f_y/1.65$ for frame members where f_y is the static yield stress for the material as listed in its specifications.
- $f_y/2.00$ for any fastener.
- deflection of frame is limited to 1/264th of the span of the supported glass.

Examples of the tables used for design of window glazing and frame loadings are given in Appendix C.

Windows may be protected by other methods. Metal window barriers may be installed, though these have the disadvantage of requiring advance warning of an attack in order to be closed before the attack occurs. Metal bars and grates and intrusion detection devices can be added to windows to delay a lone intruder. Windows can be slanted to deflect bullets that may be fired from assassins. Most window treatments will not stop a bullet from a high-powered weapon but can deflect the bullet up or down. Whatever the threat, windows often need special attention.

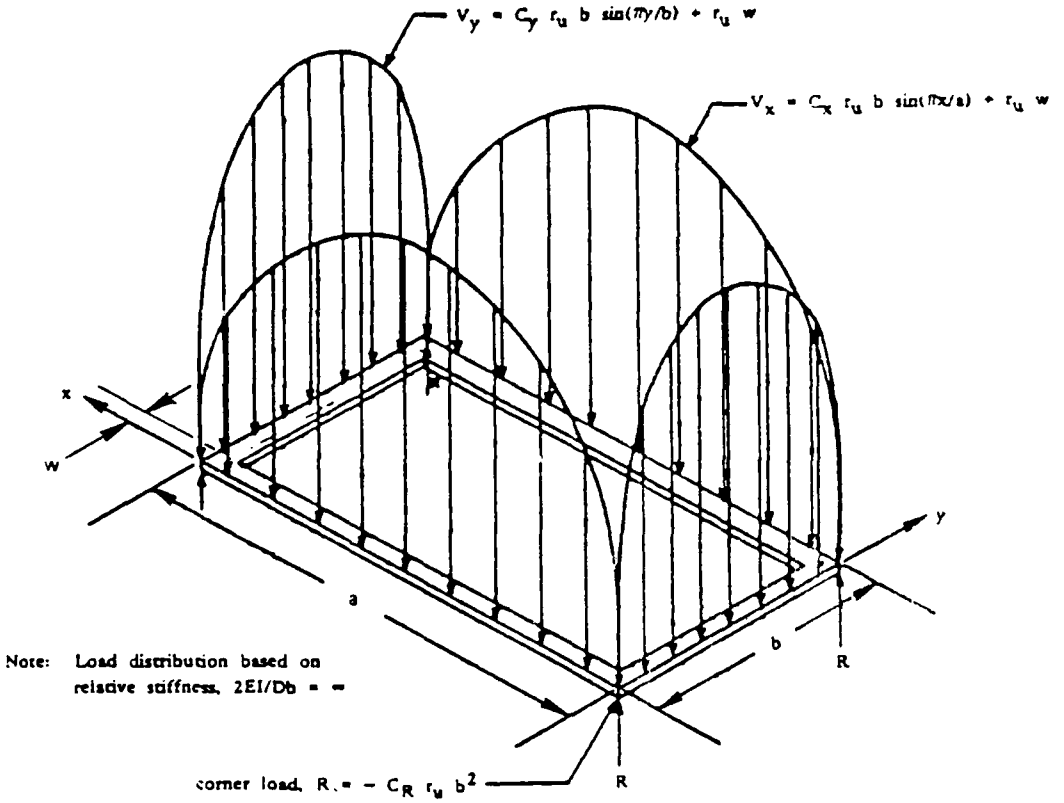


Figure 4.4: Distribution of Lateral Load on Frame
(Terrorist Vehicle Bomb Survivability Manual, p.B-5)

4.3 Utilities

If a terrorist wishes to disrupt a facility's operations, one method that may be used is to attack the facility's utilities. Protecting the utilities of the facility is often neglected and some utilities are easily disrupted by an experienced terrorist.

Vulnerable utilities include electricity, water supply, communication lines, steam, gas and even wastewater outflows. All utility outages will cause discomfort at the least. Some, such as a total power outage, could be disasterous.

Perhaps the most important utility for the majority of most facilities is electrical power. Disruption of electrical power can cause disruption of many other utilities that depend on electricity for operation. Protecting the electrical power from generation through distribution to end use is therefore very important and must be considered during any security review or design.

Designing a secure electrical system is not an easy task, especially for facilities that rely on outside sources such as power companies and host countries. A well trained terrorist will attack the weakest link in the utility system. The actual generation of power is normally relatively safe as most power plants would require a full scale attack to cause severe damage. However, there are many transmission and distribution points which could be hit that may cause power disruption.

There are many methods of protecting the power system. Redundant substations and alternate feeds are the most common type of protection. Redundancy provides an alternate route should a terrorist eliminate one route. Redundancy also provides for easier maintenance

of the system and a well-maintained system is less vulnerable than a deteriorating system. When providing alternate feed lines, they must be physically separated enough to make it impossible to knock out both feed systems with one blow (e.g., do not put both power lines on the same utility poles).

Another form of protection is to put the distribution lines underground. Although this will help to protect the lines, the above ground features are easily identified and may be targeted. Substations and overhead/underground transition points are still vulnerable. These points must be protected using physical security means and redundancy. Substations and other vulnerable points should be well lit and enclosed at least with fences with barbed wire outriggers. Locating the substations within other protected areas, such as inside the facility's perimeter, could make it less vulnerable. Installing remote intrusion detection devices could alert personnel to the possibility of an attack in progress. Using a number of different barriers that an attacker would have to get through is a delaying tactic that can help defeat a terrorist attack.

In spite of protective measures taken to prevent an attack on electrical distribution systems, they usually remain more vulnerable than the facility itself. Once electrical power is knocked out, the facility then becomes an easier target. The loss of electrical power

could cause computer systems, lighting, intrusion detection systems and even some active vehicle barriers to fail. Therefore, the importance of a source of emergency power becomes evident. Emergency generators of sufficient size and number to supply power to all critical operations and utilities should be available to rapidly respond to a power outage. The design team will need to determine which circuits should be on the emergency power circuit. Only critical items should be on the emergency circuit, such as lights, IDS, communications, etc. Fixed generators with automatic switching are preferable but portable generators can also be used. When portable generators are the source of emergency power, the facility should be equipped with quick-connect features to minimize the time the facility may be without power while hooking up the generators. Security and other sensitive systems should also be equipped with back-up battery power.[39]

The vulnerability of other utility systems should be examined and protection provided where necessary. The Naval Facilities Engineering Command publishes a *Utility Systems Vulnerability Assessment Guide* that can be used to identify key components of an utility system and to assess their vulnerability.

Communication systems should be protected in much the same manner as electrical systems. Again, redundancy and emergency power are key. The facility

should have more than one means of communication with more than one communication line to and from the building. A back-up battery powered radio link should also be available in case the terrorist is able to cut off all other communication routes.

Water supply systems are vulnerable not only to disruption but also to poisoning. Denying access as much as possible to the water distribution system and continually testing the water for quality and contaminants are the only protection means available. Again, having an emergency source of water could be important for those facilities that are isolated and could be put under siege, as many embassies could be.

Steam, gas and compressed air systems should also be protected similar to electrical power. Though these systems are often not vital to operations, they should be assessed for vulnerability and provided protection where necessary.

Another feature of some utility systems that must be taken into account is whether or not that system may provide access to the facility for an intruder. Steam tunnels, for example, could possibly offer an access route to an experienced intruder. Other utility openings in a building may provide easy access to the lone terrorist who wishes to plant a bomb. These openings should be made non-passable by covering the openings with gratings or filling them with smaller size

pipes. Intrusion detection systems could also be added if necessary.

CHAPTER V

CONCLUSIONS

"The principles for thwarting terrorist attack are much the same as those used in the medieval castle."[49]

-John Eberhard
Executive Director
Building Research Board
National Academy of Science

5.1 Summary

The design problem facing the security engineer today is a complicated one. If the design of a secure facility takes on the appearances of a prison or fortress, a small victory for the terrorists is won. Possibilities exist for making facilities and people safe from terrorism without restricting the civil liberties granted by a democratic society and without engendering a fortress mentality. The securitiy engineer must evaluate all the resources available to him to design a safe, functional and architecturally pleasing facility.

The problem of anti-terrorist engineering takes on more complications as the threat becomes more sophisticated, organized and armed with modern weapons. Weapon technology is increasing steadily; security technology must at least keep pace if security is to be maintained. Small arms fire has given way to rocket-propelled grenades and car bombs loaded with

thousands of pounds of explosives. The increased threat means that designs for secure facilities will become more complex and more expensive.

The beginning of the design process is determining the threat. Deciding what can be protected and how to protect it is the next important step. Many factors come into play and all of them need to be carefully evaluated and taken into account. Not the least of these factors is the budget. The amount of security that can be provided cannot exceed the funds available. Security can be expensive so only those areas that really need protection should be protected. Determining acceptable losses versus the cost of protection (loss versus cost factors) will help the security engineer focus his attention on the areas that need special design. It is up to the security engineer to provide the best security possible for the money available.

The first line of defense is the perimeter. If terrorists can be denied access to their target, the need to harden the target is lessoned and the chances of a successful terrorist attack are reduced. The perimeter can be protected in many ways including using terrain features, intrusion detection systems, guard forces and vehicle barriers.

The next line of defense is hardening of the structure itself. Besides using conventional hardening

methods, newer innovations such as blast barriers should be considered. When hardening a facility, the security engineer must design security into the walls, roofs, windows, doors and possibly even the floors of the facility. Utilities must also be protected.

It should be noted that this paper has assumed that an attack would be launched from the ground. Attack by air, a possible next step by terrorists as they are thwarted in their normal attacks by better security designs, pose special design problems. Also, facilities with waterfronts require special attention to avoid waterborne attack or underwater attack.

The Naval Civil Engineering Laboratory (NCEL) has taken the lead in physical security research among government agencies. The advances being made at NCEL, as well as other private and government organizations, will benefit all concerned with providing a safe and secure facility in the midst of rising terrorism.

5.2 Actions

The following actions are considered necessary to design a facility that is relatively secure from terrorist attack:

1. The threat analysis must be as accurate and complete as possible. The remainder of the security design will be based on this analysis. Ensure that all concerned, including law enforcement personnel and the customer, are involved in the preparation of the threat analysis.

2. Complete a vulnerability assessment and develop cost versus loss factors. The customer must be actively involved in determining the acceptable losses.

3. Develop different options to provide the necessary protection. Determine the cost, advantages and disadvantages of each option.

4. Integrate the security design with other systems. Fire protection, theft protection and other systems can be integrated into the design to complement each other. This "total facility control" concept can be very advantageous in more complex structures.

5. Follow-up on the system design both during and after construction and installation. This follow-up will give valuable data as to the maintainability, operation and reliability of systems used. Periodic updating of the system may be necessary as the threat changes.

The above actions will not necessarily ensure a terrorist-proof facility, especially since there probably is no such thing. However, they will enhance security design and aid in constructing a safe facility.

5.3 The Future

Terrorism is not going to disappear anytime in the near future. In fact, terrorism will probably continue to rise in future years. Stemming the tide of terrorist attacks will require the cooperation of all nations. The lethality of the attacks will probably also rise as kidnappings and disruption of operations continue to lose their popularity to the more shocking bombings and indiscriminate mass murders of innocents. Terrorists

will continue to target the United States abroad and domestic terrorism may also increase. Terrorism will gain more modern weapons in the near future and they will not be unwilling to use them.

Terrorism, therefore, will continue to provide the need for advances in security technology. The future of security engineering will see an increased role for computers, both for design and threat simulation. Electronic detection systems will be improved. Defensive systems, such as laser systems, may be developed for use on structures. New construction materials and systems such as the blast barrier will be developed to protect facilities.

Until terrorism can be reduced or eliminated, the security engineer will be called upon to provide protection as necessary for government facilities and private businesses overseas. It is a challenge that will have be to met in order to save damage costs and to save lives! Our facilities should not be fortresses, but neither should they invite terrorist attack.

APPENDIX A

VEHICLE BARRIER CRASH TESTS

Table A-1 below summarizes the current data available on vehicle crash tests as taken from the March 1986 *Terrorist Vehicle Bomb Survivability Manual* (pp. 6-1 to 6-5). The current testing is being conducted based on Navy and Department of State requirements. The criteria may be greater than required for some installations. The installation should select a system that meets the defined threat.

TABLE A-1: Vehicle Barrier Crash Tests

BARRIER	VEHICLE WEIGHT	SPEED	KINETIC ENERGY (FT-LB X 1,000)	PENETRATION[1]
Anchored Concrete Median Barrier, Not Reinforced	4,000 lb	50.0 mph	334.4	20 feet
Babcock & Wilcox Arrestor	22,000 lb	36.0 mph	953.4	No penetration
Buried Tires, 36-Ply 8-Ft Diameter, 2,000 lb Each	3,350 lb	50.5 mph	285.7	1 foot
Chain-Link Fence With Fabric Buried 2 Feet	4,050 lb	50.0 mph	338.6	Full penetration
Chain-Link Fence With 3/4-Inch-Diameter Cable	3,350 lb 4,050 lb	23.5 mph 50.6 mph	61.9 346.8	7 feet 26 feet
Chain-Link Fence With Top and Bottom Rails	3,300 lb	48.0 mph	254.3	Full penetration
Concrete Block Walls, Cores Unfilled	3,000 lb	42.0 mph	177.0	Full penetration
Concrete Block Wall With Rebar and Filled Cores	3,000 lb	21.3 mph	45.5	Full penetration

TABLE A-1 (continued)

BARRIER	VEHICLE WEIGHT	SPEED	KINETIC ENERGY (FT-LB X 1,000)	PENETRATION[1]
Delta TT203 (Replaced by TT210)	15,000 lb 10,000 lb	30.0 mph 50.0 mph	451.4 836.0	No penetration No penetration
Delta TT207, 30 Inches High	6,000 lb 18,000 lb	50.0 mph 30.0 mph	501.6 541.7	27 feet 29 feet (dump bed only)
Delta TT207S, 38 Inches High	14,815 lb	49.9 mph	1,233.6	0.75 foot
Delta TT210, 24-Inch Bollard	15,180 lb 10,183 lb	32.0 mph 40.0 mph	513.6 535.0	12.2 feet No penetration
Delta TT212	10,100 lb	17.0 mph	97.6	No penetration
Delta TT241, 19 Inches High, 17 Inches Wide	6,000 lb	29.0 mph	168.7	82 feet
Double Swing Gate With Latch and Cane Bolt	4,000 lb	50.0 mph	334.4	Full penetration
Dual Post, 5/8-Inch Cable	4,500 lb	20.0 mph	60.2	Full penetration
Dual Post, 3/4-Inch Cable	4,500 lb	20.0 mph	60.2	2 feet
Dual Post, 3/4-Inch Cable	4,500 lb	39.0 mph	228.9	Full penetration
Dual Post, 3/4-Inch Cable	4,500 lb	47.0 mph	332.4	Full penetration
8-Inch Bollard System	15,000 lb	43.5 mph	949.2	19.6 feet
8-Inch Bollard System	15,000 lb	47.0 mph	1,108.0	No penetration
Entwistle Dragnet	1,460 lb	42.0 mph	86.1	10.2 feet
Entwistle Dragnet	1,620 lb	48.0 mph	124.8	13.8 feet

TABLE A-1 (continued)

BARRIER	VEHICLE WEIGHT	SPEED	KINETIC ENERGY (FT-LB X 1,000)	PENETRATION[1]
Entwistle Dragnet	3,760 lb	56.0 mph	394.3	26.3 feet
Entwistle Dragnet	3,880 lb	62.0 mph	498.7	Greater than 30 feet
Entwistle Dragnet	4,300 lb	60.0 mph	517.7	19.4 feet
Entwistle Dragnet	4,520 lb	54.0 mph	440.7	23.5 feet
Frontier Mac-H10, 32 Inches High, 120 Inches Long	18,000 lb 20,000 lb	35.0 mph 41.0 mph	737.4 1,124.3	1 foot 56 feet
Nasatka MSBII	14,980 lb	50.3 mph	1,267.4	No penetration
Reinforced Concrete Wall, 6 Inches Thick	3,000 lb	39.6 mph	157.31	No penetration
Robot SCB Crash Beam	4,500 lb	23.0 mph	79.6	4 feet
Rewes Security Gate	10,000 lb	50.0 mph	836.0	4.2 feet
Single Buried Concrete-Filled 8-Inch-Diameter Schedule 40 Pipe	4,500 lb	30.0 mph	135.4	3 feet
Single Swing Gate With Latch and Locked Chain	4,000 lb	50.0 mph	334.4	Full penetration
SNLA[2] Crash Beam	22,000 lb	36.3 mph	969.4	6 feet
SNLA[2] Crash Beam	22,000 lb	43.0 mph	1,360.3	13 feet
SNLA[2], V-Fence With Rock and Pole Fill	3,800 lb	52.0 mph	343.6	8 feet
Steel Cable Barriers, Two 3/4-Inch Cables	4,000 lb	52.0 mph	361.7	13 feet
Tiretrap Devastator	11,500 lb	34.0 mph	444.6	8.5 feet

TABLE A-1 (continued)

BARRIER	VEHICLE WEIGHT	SPEED	KINETIC ENERGY (FT-LB X 1,000)	PENETRATION[1]
Twin T-Beam Wall	3,000 lb	42.5 mph	181.2	Full penetration
Western Portapungi	14,980 lb	39.8 mph	793.5	40 feet

[1]Full penetration may mean the vehicle passed through the barrier and was still capable of movement and control, as is the case of the chain-link fence, or it may mean that a major portion of the vehicle and/or its payload passed through the barrier, but the vehicle was essentially destroyed and incapable of control or self movement. Actual test results (many of which are summarized in chapters 7 and 8) should be reviewed when definitive results are desired.

[2]Sandia National Laboratory, Albuquerque

APPENDIX B

EXPLOSIVE PRESSURES

Table B-1 shows peak pressures and durations for specific charge weights (TNT equivalency) and stand-off distances. The tables are for both reflected and incident pressure. Windows and walls that are around a corner from the direction of an expected blast may be designed for incident pressures. Table B-1 is taken from the March 1983 *NAVFAC DM 13.1* (pp. 289-291).

TABLE B-1:Pressures and Durations of Specified Bomb Threats

Charge Weight, W = 4,000 lbs (TNT Equivalency)				
Stand-off Distance	Reflected Pressure		Incident Pressure	
	Peak Pressure	Duration	Peak Pressure	Duration
R (ft)	P_r (psi)	T_r (msec)	P_o (psi)	T_o (msec)
50	646	3.6	122	6.3
75	173	8.0	48.2	10.1
100	74.0	13.3	23.8	16.0
125	42.5	17.8	15.1	20.7
150	27.0	22.6	10.5	25.4
200	14.6	30.3	6.3	32.9
300	7.1	40.3	3.2	44.9
500	3.4	49.6	1.6	54.9

TABLE B-1 (continued)

Charge Weight, W = 1,000 lbs (TNT Equivalency)				
Stand-off Distance	Reflected Pressure		Incident Pressure	
	Peak Pressure	Duration	Peak Pressure	Duration
R (ft)	P_r (psi)	T_r (msec)	P_o (psi)	T_o (msec)
50	140	5.7	41.5	6.9
75	48	10.5	16.7	12.3
100	23.4	15.3	9.4	17.0
125	14.9	18.8	6.4	20.5
150	10.3	22.3	4.7	23.8
200	6.4	26.5	3.0	28.6
300	3.7	30.2	1.7	34.1
500	1.7	37.6	0.80	43.7

Charge Weight, W = 300 lbs (TNT Equivalency)				
Stand-off Distance	Reflected Pressure		Incident Pressure	
	Peak Pressure	Duration	Peak Pressure	Duration
R (ft)	P_r (psi)	T_r (msec)	P_o (psi)	T_o (msec)
25	391.5	2.0	86.3	3.1
50	49.5	7.0	16.9	8.1
75	18.6	11.4	7.74	12.5
100	10.4	14.9	4.73	15.9
125	7.25	16.8	3.33	18.4
150	5.55	18.2	2.57	20.0
200	3.72	20.2	1.75	22.2
300	2.04	23.7	1.00	26.2
500	1.06	27.3	0.53	30.7

TABLE B-1 (continued)

Charge Weight, W = 100 lbs (TNT Equivalency)				
Stand-off Distance	Reflected Pressure		Incident Pressure	
	Peak Pressure	Duration	Peak Pressure	Duration
R (ft)	P_r (psi)	T_r (msec)	P_o (psi)	T_o (msec)
25	114	3.0	34.7	3.6
50	20.2	7.6	8.30	8.4
75	9.14	10.8	4.20	11.6
100	5.86	12.4	2.71	13.7
125	4.29	13.5	2.02	14.8
150	3.30	14.5	1.56	16.0
200	2.16	16.2	1.05	18.0
300	1.27	18.1	0.64	20.2

Charge Weight, W = 30 lbs (TNT Equivalency)				
Stand-off Distance	Reflected Pressure		Incident Pressure	
	Peak Pressure	Duration	Peak Pressure	Duration
R (ft)	P_r (psi)	T_r (msec)	P_o (psi)	T_o (msec)
10	606	0.70	117	1.2
25	40.3	3.50	14.6	4.1
50	9.20	7.20	4.21	7.7
75	5.00	8.70	2.33	9.5
100	3.32	9.70	1.57	10.7
125	2.38	10.6	1.14	11.9
150	1.83	11.2	0.92	12.2
200	1.27	12.2	0.64	13.5

APPENDIX C

WINDOW DESIGN TABLES

Table C-1 is an example of a table that can be used to determine the thickness for laminated thermally tempered glass. This table, and others for different charge weights and aspect ratios, can be found in Appendix B of the *Terrorist Vehicle Bomb Survivability Manual.* To find the required thickness, use the proper table for charge weight and aspect ratio (4000 lbs and 1.25 respectively shown in table C-1). Enter the table with the plate dimensions (inches) and go across to the desired stand-off distance (feet). Read the glazing thickness in inches. Round up to normally manufactured glazing thicknesses. Use next larger window dimensions and next smaller stand-off distance if desired numbers are not in the tables.

Table C-1:Glazing Thicknesses

Plate Dimension (in.)		Range (ft)							
B	A	50	75	100	125	150	200	300	500
12.000	15.000	2.050	1.085	0.706	0.592	0.426	0.314	0.204	0.124
14.000	17.500	2.385	1.263	0.811	0.681	0.490	0.360	0.237	0.144
16.000	20.000	2.717	1.440	0.924	0.776	0.559	0.411	0.270	0.165
18.000	22.500	3.046	1.616	1.038	0.872	0.627	0.461	0.303	0.184
20.000	25.000	3.374	1.790	1.150	0.967	0.695	0.511	0.335	0.204
22.000	27.500	3.701	1.963	1.261	1.061	0.763	0.561	0.366	0.224
24.000	30.000	4.024	2.136	1.372	1.154	0.830	0.610	0.398	0.244
26.000	32.500	4.333	2.309	1.483	1.248	0.897	0.659	0.431	0.263
28.000	35.000	4.640	2.479	1.594	1.341	0.964	0.708	0.465	0.282
30.000	37.500	4.945	2.643	1.703	1.433	1.030	0.757	0.498	0.300
32.000	40.000	5.248	2.805	1.807	1.526	1.094	0.804	0.531	0.319
34.000	42.500	5.549	2.966	1.912	1.616	1.157	0.850	0.564	0.337
36.000	45.000	5.849	3.127	2.015	1.704	1.220	0.896	0.597	0.355
38.000	47.500	6.161	3.287	2.118	1.791	1.282	0.942	0.630	0.374
40.000	50.000	6.475	3.445	2.221	1.878	1.344	0.988	0.663	0.393
42.000	52.500	6.788	3.604	2.323	1.965	1.406	1.033	0.697	0.412
44.000	55.000	7.100	3.768	2.424	2.051	1.468	1.078	0.730	0.431
46.000	57.500	7.412	3.933	2.527	2.136	1.529	1.123	0.763	0.449
48.000	60.000	7.724	4.099	2.634	2.222	1.592	1.170	0.796	0.468
50.000	62.500	8.035	4.264	2.740	2.307	1.656	1.218	0.829	0.487
52.000	65.000	8.346	4.429	2.846	2.394	1.720	1.265	0.861	0.506

Table C-2 lists the static frame design load factor, r_u, as a function of window dimensions and stand-off range. These tables are used in the same manner as table C-1 and are also found in the *Terrorist Vehicle Bomb Survivability Manual.* More tables are available for different charge weights and aspect ratios. The factor r_u is then used to calculate expected window loads as described in section 4.2.3.

TABLE C-2:Static Frame Design Load, r_u (psi)

STATIC FRAME DESIGN LOAD (PSI)
CHARGE WEIGHT = 4000 LBS

ASPECT RATIO =1.00

PLATE DIMENSION (IN)		RANGE (FT)							
B	A	50	75	100	125	150	200	300	500
12.000	12.000	1253.64	351.63	148.39	104.14	54.01	29.29	15.35	8.61
14.000	14.000	1246.98	349.39	143.98	104.08	52.67	28.52	14.85	8.59
16.000	16.000	1240.95	347.71	143.21	101.00	52.33	28.43	14.79	8.58
18.000	18.000	1232.52	346.41	142.61	100.77	52.26	28.22	14.74	8.48
20.000	20.000	1224.12	344.48	142.14	100.34	52.03	28.07	14.71	8.48
22.000	22.000	1217.27	342.50	141.49	99.99	51.68	27.95	14.63	8.41
24.000	24.000	1211.58	340.86	140.71	99.50	51.40	27.86	14.58	8.36
26.000	26.000	1201.01	339.13	140.06	99.09	51.16	27.69	14.54	8.37
28.000	28.000	1187.86	337.65	139.29	98.56	50.95	27.54	14.48	8.32
30.000	30.000	1174.88	335.49	138.82	98.27	50.77	27.42	14.45	8.23
32.000	32.000	1163.57	332.25	137.88	97.86	50.51	27.31	14.38	8.15
34.000	34.000	1152.21	329.14	136.73	97.51	50.08	27.09	14.31	8.08
36.000	36.000	1142.16	326.39	135.55	96.93	49.69	26.89	14.23	8.06
38.000	38.000	1131.93	323.48	134.35	96.16	49.27	26.66	14.15	8.00
40.000	40.000	1127.58	320.88	133.28	95.36	48.88	26.45	14.09	7.91
42.000	42.000	1124.04	318.53	132.31	94.64	48.46	26.21	14.03	7.87
44.000	44.000	1120.46	316.21	131.31	93.98	48.15	26.04	13.97	7.83
46.000	46.000	1117.55	314.66	130.40	93.29	47.79	25.84	13.90	7.82
48.000	48.000	1114.21	313.76	129.57	92.65	47.47	25.66	13.87	7.79
50.000	50.000	1111.47	312.94	129.24	92.07	47.24	25.54	13.87	7.79
52.000	52.000	1108.63	312.19	128.84	91.53	47.09	25.50	13.84	7.76
54.000	54.000	1105.71	311.33	128.56	91.03	47.01	25.43	13.82	7.73
56.000	56.000	1103.00	310.69	128.21	90.82	46.88	25.37	13.80	7.73
58.000	58.000	1100.48	309.95	127.98	90.62	46.76	25.30	13.78	7.71
60.000	60.000	1097.60	309.25	127.67	90.36	46.70	25.25	13.76	7.69

APPENDIX D

PHYSICAL SECURITY REQUIREMENTS ASSESSMENT METHODOLOGY

D.1 Introduction.

Computer applications are now being developed for security engineering. One such program that is being developed by the Naval Civil Engineering Laboratory is the Physical Security Requirements Assessment Methodology (PSRAM). PSRAM has been developed as a design aid for improving physical security at existing naval bases and for new construction.

PSRAM currently examines three alternatives for relative cost-effectivieness: structural hardening, intrusion detection systems (IDS), and security personnel. The most cost-effective mixture of these alternatives is identified by PSRAM through a repetitive iteration process. PSRAM allows two basic outputs, the confidence of intercepting an intruder and the 25 year life cycle cost of the security system. PSRAM also allows the user to evaluate a specified security system or automatically search for the most cost-effective option.

D.2 Inputs

Inputs to PSRAM by the user include the layout of the road network, descriptions of current facilities

(facility numbers, perimeters in feet and the locations). This data is then stored on disk for use as necessary. New inputs include the location of the new facility under consideration, the perimeter of the facility that must be secured (in feet), the design threat, descriptions of any structural barriers and descriptions of any IDS that may be included. Ranges can be specified for the latter two items and PSRAM will then find the most cost-effective IDS and hardening options.

PSRAM contains over 260 construction options for structural hardening. Table D-1 contains a sample of some of the options. The costs listed in table D-1 are the default costs and are based on the McGraw-Hill series of estimating manuals. Table D-2 shows IDS sensor type options available in PSRAM and the associated default costs. The user may design with or without any of the type of sensors listed in Table D-2. The user may also specify 25 year life cycle costs of IDS or structural hardening in which case the default costs will not be used.

The number and type of security guards can also be inputted. If guards are not specified by the user, PSRAM will search for the most cost-effective guard mix, either roving or fixed.

TABLE D-1: Facility Construction Options

Building Component	Construction Type		Default Unit Life Cycle Costs (25 yr FY 83 $ per sq.ft)	Attack Reference Codes
	FEPAS No.	Description		
Windows	1.	Round bars 3/8" diameter.	8.65	X-1 through X-
	2.	Round bars 1/2" diameter.	12.95	X-4 through X-
	3.	1 1/4" x 3/8" flat bars and 1/2" rods.	27.35	X-7 through X-
Doors	4.	16 gauge hollow metal.	17.30	D-10 through D-
	5.	12 gauge hollow metal.	26.65	D-18 through D-
	16.	Magazine door.	57.60	D-52 through D-
Walls	6.	Wood frame 1" T&G on 16" studs.	5.00	W-25 through W-
	7.	Wood frame 1" T&G over 1/2" plywood.	6.70	W-29 through W-
	8.	Stucco.	5.20	W-34 through W-
	9.	Reinforced concrete 12" thick.	13.25	W-37 through W-
	10.	Reinforced concrete 8" thick.	8.90	W-39 through W-
	11.	Reinforced concrete 6" thick.	8.15	W-42
	12.	concrete block 8" thick, filled and reinforced.	5.45	W-43 through W-
	13.	Concrete block 8" thick, filled.	5.05	W-47
	14.	Concrete block 8" thick, hollow.	3.90	W-48
	15.	8" brick.	9.75	W-49 through W-
	17.	Reinforced concrete 12" thick, 24" earth cover.	15.65	W-64 through W-
	18.	Reinforced concrete 8" thick, 24" earth cover.	11.30	W-66 through W-
	19.	Reinforced concrete 6" thick, 24" earth cover.	10.55	W-69
Roof	20.	Wood frame 1" T&G over 1/2" plywood.	6.70	R-70 through R-
	21.	Reinforced concrete 12" thick.	20.00	R-75 through R-
	22.	Reinforced concrete 8" thick.	11.20	R-77 through R-
	23.	Reinforced concrete 6" thick.	8.20	R-80
Floor	24.	Reinforced concrete 8" thick.	3.90	N/A

N/A = Not Applicable

TABLE D-2: IDS Sensor Type Options

Observable	Default 25 yr Life Cycle Unit Cost (FY83 $ per sq. ft)
Noise	6.59
Smoke	6.59
Heat	22.58
Light	22.58
Vibration	55.10
Motion	14.64

Table D-3 shows the threat inputs that may be specified by the user. The user first identifies the level of attack tools the threat may use (table D-3). The skill level then may also be specified as "skilled", "skilled with tool penalty" (tools used require time to set up or are bulky), "unskilled" and "unskilled with tool penalty." The user also may input a penetration opening size required, 96 square inches is nominal for man-sized openings but if destruction of the facility is the threat's objective, a smaller opening may be required.

TABLE D-3: Design Threat Characteristics

Threat Level	Number of People	Tools	Type of Facilities Affected	Probability of Losses	Total Cost of Losses*	Operational Impact
Low Level	1	pry bar bolt cutter body force	commissary administration buildings covered storage open storage family housing maintenance shop dormitory	high	high	low
Mid Level	1-3	pry bar bolt cutter other hand tools	covered storage supply buildings maintenance shops open storage administration Navy exchange operations buildings	high	moderate	moderate
High Level Terrorist (CONUS)	**	car bombs man carried bombs letter bombs small arms	command facilities security facilities fuel tanks parked aircraft computer facilities AA&E facilities	low (potential threat-no loss history experience)	moderate	moderate
Terrorist (OCONUS)	**	car bombs man carried bombs letter bombs small arms rockets & grenades hand & power tools	nuclear facilities AA&E facilities computer facilities command facilities fuel tanks parked aircraft	high (immediate threat)	high	high (operational & political impact)
Saboteur (CONUS)	**	hand & power tools explosives	classified areas communication centers nuclear facilities AA&E facilities utilities fuel tanks	low (in stable peace-time environment-threat in place when hostilities commence	moderate	high
Saboteur (OCONUS)	**	hand & power tools explosives small arms rockets & grenades	nuclear facilities AA&E facilities communication centers computer facilities maintenance shops fuel tanks aircraft & missiles	moderate	high	high
Nuclear & Environmental Activists	**	hand tools battering tools	nuclear facilities computing centers shipyards weapon stations command centers	high	low	low

*Loss costs include material replacement costs, operational downtime costs, facility repair costs, investigative costs, and deterent costs.

**Defined in OPNAVINST C-5510.83E

D.3 Outputs

The PSRAM system will print outputs in several forms. The options selected by PSRAM may be sorted by minimum cost, maximum confidence of intercept or minimum cost per confidence level ratio. The printouts will include construction type, recommended sensors, the confidence of intercept for each building component (walls, roofs, floors, doors and windows), the number and type of guards and the system 25 year life cycle cost. If the user is using the system to evaluate a specific security system, a more detailed printout is produced.

D.4 Example Printout

The following four pages contain a sample printout of a PSRAM run. The building analyzed in this run is an administration building to be constructed at the new home port in Everett, Washington. The first pages show some of the inputs that were included in this run. Note that the threat level inputted was level 4 with a "skilled" threat. No IDS sensors were used. Limits on life-cycle cost were inputted only for the total cost.

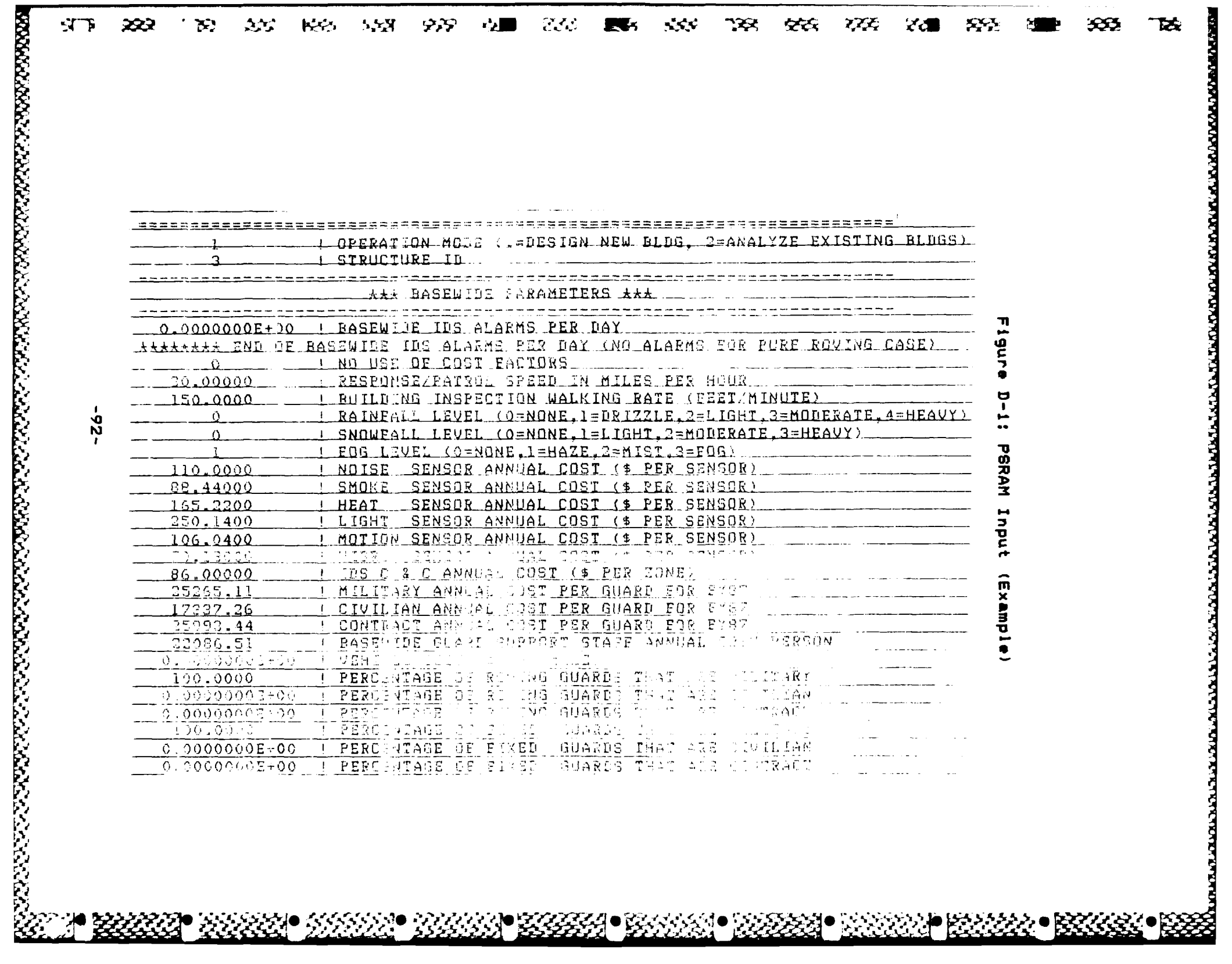
The output was sorted by confidence of intercept. The "X-S#" (or cross-section number) columns shown on the output refer to tables in the PSRAM users manual that correlate the number to a particular type of construction cross-section. For example, the 39 for

wall cross-sections in the example printout can be found from table D-4 to be a 2x4" studs with 2" wood siding wall, which is then described in more detail in table D-5. The same procedure results in determining the optimum construction options for each building component as determined by PSRAM. The example output also shows the optimum mix of guards (in this case 3 roving guards) and the total costs associated with each option.

D.5 Summary

PSRAM is already being used to evaluate new construction, as shown in the example printout. It should save time, effort and money when designing secure facilities. It is currently limited in its use in several ways, but development of the program is continuing and improvements are being made. For example, it currently cannot handle options for high terrorist or military threat that include explosives. However, a high threat submodel is being developed that should eventually solve this limitation. PSRAM, and other programs like it, will become invaluable to the security engineer designing against a multitude of threats with many options available.

(The material for this appendix was taken from "A Computer System For Analyzing and Designing Physical Security for Naval Shore Facilities" an Executive Summary by L.M. Pietrzak and G.A. Johanson, January 1986, prepared by the Mission Research Corporation)



```
=============================================================================
        1          ! OPERATION MODE (1=DESIGN NEW BLDG, 2=ANALYZE EXISTING BLDGS)
        3          ! STRUCTURE ID
-----------------------------------------------------------------------------
                        *** BASEWIDE PARAMETERS ***
-----------------------------------------------------------------------------
 0.0000000E+00     ! BASEWIDE IDS ALARMS PER DAY
********** END OF BASEWIDE IDS ALARMS PER DAY (NO ALARMS FOR PURE ROVING CASE)
        0          ! NO USE OF COST FACTORS
    30.00000       ! RESPONSE/PATROL SPEED IN MILES PER HOUR
    150.0000       ! BUILDING INSPECTION WALKING RATE (FEET/MINUTE)
        0          ! RAINFALL LEVEL (0=NONE,1=DRIZZLE,2=LIGHT,3=MODERATE,4=HEAVY)
        0          ! SNOWFALL LEVEL (0=NONE,1=LIGHT,2=MODERATE,3=HEAVY)
        1          ! FOG LEVEL (0=NONE,1=HAZE,2=MIST,3=FOG)
    110.0000       ! NOISE  SENSOR ANNUAL COST ($ PER SENSOR)
    88.44000       ! SMOKE  SENSOR ANNUAL COST ($ PER SENSOR)
    165.2200       ! HEAT   SENSOR ANNUAL COST ($ PER SENSOR)
    250.1400       ! LIGHT  SENSOR ANNUAL COST ($ PER SENSOR)
    106.0400       ! MOTION SENSOR ANNUAL COST ($ PER SENSOR)
    [illegible]    ! [illegible]
    86.00000       ! IDS C & C ANNUAL COST ($ PER ZONE)
    25265.11       ! MILITARY ANNUAL COST PER GUARD FOR FY87
    17237.26       ! CIVILIAN ANNUAL COST PER GUARD FOR FY87
    25293.44       ! CONTRACT ANNUAL COST PER GUARD FOR FY87
    22086.51       ! BASEWIDE CLASS SUPPORT STAFF ANNUAL [illegible] PERSON
 0.[illegible]     ! VEH[illegible]
    100.0000       ! PERCENTAGE OF ROVING GUARDS THAT ARE MILITARY
 0.0000000E+00     ! PERCENTAGE OF ROVING GUARDS THAT ARE CIVILIAN
 0.0000000E+00     ! PERCENTAGE OF ROVING GUARDS THAT ARE CONTRACT
    100.00         ! PERCENTAGE OF FIXED GUARDS THAT ARE MILITARY
 0.0000000E+00     ! PERCENTAGE OF FIXED GUARDS THAT ARE CIVILIAN
 0.0000000E+00     ! PERCENTAGE OF FIXED GUARDS THAT ARE CONTRACT
```

Figure D-1: PSRAM Input (Example)

```
  100.0000          ! PERCENTAGE OF ROVING GUARDS WITH 24 HOUR SHIFTS
0.0000000E+00       ! PERCENTAGE OF ROVING GUARDS WITH 16 HOUR SHIFTS
0.0000000E+00       ! PERCENTAGE OF ROVING GUARDS WITH  8 HOUR SHIFTS
  100.0000          ! PERCENTAGE OF FIXED  GUARDS WITH 24 HOUR SHIFTS
0.0000000E+00       ! PERCENTAGE OF FIXED  GUARDS WITH 16 HOUR SHIFTS
0.0000000E+00       ! PERCENTAGE OF FIXED  GUARDS WITH  8 HOUR SHIFTS
          1         ! NUMBER OF GUARD SUPPORT STAFF PER SHIFT
          1         ! MINIMUM NUMBER OF ROVING GUARDS
          2         ! MAXIMUM NUMBER OF ROVING GUARDS
-------------------------------------------------------------------------
                    *** BUILDING SPECIFIC PARAMETERS ***
-------------------------------------------------------------------------
       1987         ! FISCAL YEAR OF CONSTRUCTION
         25         ! LIFE CYCLE OF THE BUILDING
          4         ! ATTACK THREAT LEVEL
          1         ! ATTACK TIME OPTION (1=OPTIMUM,2=+SKILL PENALTY,3=+TOOL PENALTY,
   96.00000         ! ATTACK MINIMUM HOLE SIZE (INCHES)
          1         ! WINDOWS USED (0=NO, 1=YES)
          2         ! FLOORS [illegible] (0=NO, 1=YES)
          1         ! DESIGN FOR EXT, INT, (OR BOTH) SHELL SECURITY (0=NO INT,1=SAME,
          1         ! NUMBER OF SERIAL DOORS PER DOOR LOCATION
         10         ! TOTAL NUMBER OF EXTERIOR DOOR LOCATIONS
   [illegible]      ! AVERAGE HEIGHT OF SECURED AREA IN FT
                    ! NUMBER OF [illegible] WINDOWS PER WINDOW LOCATION
                    ! CONSTRUCTION FILTER CHOICE (1=FREQUENCY,2=TYPE/CLASS)
                    ! WALL COMPONENT NUMBER OF FILTER LIST ENTRIES
   -99              ! [illegible] NUMBER OF FILTER LIST ENTRIES
   [illegible]      ! FLOOR COMPONENT NUMBER OF FILTER LIST ENTRIES
   -1[illegible]    ! DOOR [illegible] NUMBER OF FILTER LIST ENTRIES
```

Figure D-1 (continued)

```
     1          ! WINDOW COMPONENT NUMBER OF FILTER LIST ENTRIES
-201
     0          ! SENSORS USED (0=NO, 1=YES)
     0          ! MINIMUM NUMBER OF FIXED GUARDS
     0          ! MAXIMUM NUMBER OF FIXED GUARDS
0.0000000E+00   ! TOTAL LIFECYCLE COST LOWER LIMIT
0.5000000E+08   ! TOTAL LIFECYCLE COST UPPER LIMIT
0.0000000E+00   ! LIFECYCLE GUARD COST LOWER LIMIT
0.0000000E+00   ! LIFECYCLE GUARD COST UPPER LIMIT
0.0000000E+00   ! LIFECYCLE HARDENING COST LOWER LIMIT
0.0000000E+00   ! LIFECYCLE HARDENING COST UPPER LIMIT
0.0000000E+00   ! LIFECYCLE SENSOR COST LOWER LIMIT
0.0000000E+00   ! LIFECYCLE SENSOR COST UPPER LIMIT
0.0000000E+00   ! CONFIDENCE OF INTERCEPT IN TIME LOWER LIMIT
 100.0000       ! CONFIDENCE OF INTERCEPT IN TIME UPPER LIMIT
     0          ! SORT OPTIONS BY LOWEST COST     (0=NO, 1=YES)
     1          ! SORT OPTIONS BY HIGHEST CI      (0=NO, 1=YES)
     0          ! SORT OPTIONS BY LOWEST COST/CI (0=NO, 1=YES)
   102          ! BRIEF OUTPUT FORMAT #1 (0=NO, >0=CASE LIMIT)
   102          ! BRIEF OUTPUT FORMAT #2 (0=NO, >0=CASE LIMIT)
     0          ! BRIEF OUTPUT FORMAT #3 (0=NO, >0=CASE LIMIT)
     2          ! FULL OUTPUT FORMAT     (0=NO, >0=CASE LIMIT)
```

Figure D-1 (continued)

Figure D-2: PSRAM Output (Example)

SORTED ON HIGHEST CONFIDENCE OF INTERCEPT SHELL CASE: EXT

OPTION	WALL X-S#	WALL CI	ROOF X-S#	ROOF CI	FLOOR X-S#	FLOOR CI	DOOR X-S#
1	39	100	165	100	156	N/A	209
2	39	100	165	100	156	N/A	223
3	39	56	165	43	156	N/A	223
4	39	56	165	43	156	N/A	209
5	39	0	165	0	156	N/A	223
6	39	0	165	0	156	N/A	209

ONLY. INTERIOR NOT CONSIDERED.

TOTAL 25 YEAR LIFECYCLE COST	CONSTRUCTION LIFECYCLE COST	SENSOR LIFECYCLE COST	GUARDS LIFECYCLE COST
1477820	342503	0	113531
1441025	305708	0	113531
1147979	305708	0	842271
1184774	342503	0	842271
854933	305708	0	549225
891728	342503	0	549225

SORTED ON HIGHEST CONFIDENCE OF INTERCEPT SHELL CASE: EXTERIOR

OPTION	MINIMUM CONFIDENCE OF INTERCEPT IN TIME	★★★★ CONFIDENCE OF INTERCEPT ★★★★★ WALL	ROOF	FLOOR	DOOR	WINDOW
1	99	100	100	N/A	100	99
2	98	100	100	N/A	98	98
3	20	56	43	N/A	39	20
4	20	56	43	N/A	53	20
5	0	0	0	N/A	0	0
6	0	0	0	N/A	0	0

ONLY. INTERIOR NOT CONSIDERED.

WINDOWS X-S#	WINDOWS CI	SENSORS VIBRATION	SENSORS INTERIOR	GUARDS FIX	GUARDS ROV	TOTAL COST
201	99			0	3	147[illegible]
201	99			0	2	144[illegible]
201	20			0	2	114[illegible]
201	20			0	2	118[illegible]
201	0			0	1	854[illegible]
201	0			0	1	891[illegible]

Table D-4: Cross Sections Contained in PSRAM
(Example)

CROSS-SECTION NUMBER	BUILDING COMPONENT	TYPE	UNIT COST $/SQ.FT.	ABBREVIATED NAME
1	WALL	1	12.21	8"CONC#4 8" EACH FACE REBAR
2	WALL	3	7.76	8" #4 REBAR EVRY CRS MF
3	WALL	9	12.25	8" BRICK
4	WALL	1	15.07	12"CONC#6 12"EACHFACE REBAR
23	WALL	1	14.02	8"CONC #6 6" REBAR
24	WALL	1	19.47	12"CONC#6 6"EACH FACE REBAR
25	WALL	1	25.47	18"CONC#6 6" 3 LAYERS REBAR
26	WALL	1	31.47	24"CONC#6 6" 4 LAYERS REBAR
27	WALL	1	43.35	36"CONC#6 6" 6 LAYERS REBAR
28	WALL	1	55.29	48"CONC#8 6" 8 LAYERS REBAR
29	WALL	1	20.69	12"CONC#6 16"V 6"H 5/16" EM
30	WALL	1	22.28	18"CONC#6 16"V 6"H 5/16" EM
31	WALL	1	23.87	24"CONC#6 16"V 6"H 5/16" EM
32	WALL	1	26.94	36"CONC#6 16"V 6"H 5/16" EM
33	WALL	1	12.18	4"CONC #5 5" REBAR EACH WAY
34	WALL	2	12.80	4"FIB CONC #5 5" REBAR
37	WALL	1	13.28	8"CONC #5 5" REBAR
39	WALL	6	6.16	2X4"STUDS 2"SIDING
42	WALL	4	13,85	1"BRK 8"CMU #5REBAR MORTAR
45	WALL	1	11.82	8"CONC #6 12" REBAR
47	WALL	3	13.64	8" CMU #8 REBAR MORTAR
48	WALL	4	14.63	8" CMU MORTAR 3" FIB CONC
49	WALL	4	13.36	3/4"PLY 1"FM EM 8" CMU
50	WALL	4	8.39	1" FOAM DMPL 8" CMU
51	WALL	4	16.64	4"BRICK 4"CMU 3/4"EM 4"CMU
52	WALL	4	11.27	8" CMU EXP METAL 4"CMU
53	WALL	4	13.67	8"CMU WIRE FBRC 4"FERROCMNT
54	WALL	4	16.45	8"CMU 2 LINK FENCE EM FC
55	WALL	7	13.86	BS F SHT STD GYP PLY SM
56	WALL	7	12.33	BS F SHT STD GYP PLY EM PLY
57	WALL	7	17.03	BS F SHT STD GYP WWF FC
58	WALL	6	9.74	BS #15 FELT 1X6SHT 3/8"PLY
59	WALL	1	12.67	8"CONC #5 6" REBAR
60	WALL	1	10.60	8"CONC#2 6" EACH FACE REBAR
61	WALL	7	10.64	GYP STD GYP SSTD MS
62	WALL	7	7.53	GYP STD GYP SSTD MS
72	WALL	5	17.81	10GA SM EM 1/2"FM 10GA SM
73	WALL	5	20.12	10GA SM RM EM 1.8"OAK 10GA
74	WALL	5	18.23	1/4"SP 1 1/2"OAK 3"FM 10GA
75	WALL	5	14.13	1/4"SP 20GA SM 3"FM 1"PLY
96	WALL	3	5.64	8" CMU #3 REBAR
97	WALL	4	12.39	8" CMU 1/4" EXP METAL
98	WALL	4	8.29	8" CMU 1.5" PLYWOOD
99	WALL	4	8.29	8" CMU 3/4" PLY MAT 3/4"PLY
110	WALL	1	16.36	4"CONC. STEELMESH 6X6X1/4"
111	WALL	1	11.57	4"CONC #5 6" REBAR EACH WAY
112	WALL	1	10.56	6"CONC #4 8" REBAR EACH WAY
113	WALL	1	12.67	8"CONC #5 6" REBAR
114	WALL	1	14.02	9"CONC #6 6" REBAR

Table D-5: Cross Section Descriptions Contained in PSRAM (Example)

WALLS (CONT.)

NO.	CROSS-SECT. NO.	ABBREVIATION	DESCRIPTION
73	226	9GA SP 3/4"PLY 9GA SP	ASTM 607 HS, 9ga, front plywood, 3/4", center ASTM 607 HS, 9ga, back
77	227	9GA 90#MAT PLY 90#MAT 9GA	ASTM 607 HS, 9ga, front roof mat, 90#, 2nd plywood, 3/4", 3rd roof mat, 90#, 4th ASTM 607 HS, 9ga, back
74	312	0.105" SP .5 PLEX SP PLEX SP	ASTM A-607 steel, 0.105, 1st plex, 0.5, 2nd ASTM A-607 steel, 0.105, 3rd plex, 0.5, 4th ASTM A-607 steel, 0.105, 5th
75	313	0.105" SP .5 LEX SP LEX SP	ASTM A-607 steel, 0.105", 1st lexan, 0.5", 2nd ASTM A-607 steel, 0.105", 3rd lexan, 0.5", 4th ASTM A-607 steel, 0.105", 5th
76	314	0.25 SS .5 PLEX SP	SS, 0.25", 1st plex, 0.5", 2nd ASTM A607 steel, 0.105", 3rd
WOOD			
77	39	2X4"STUDS 2"SIDING	studs, 2x4" wood siding, 2", double planking over studs
78	58	BS #15 FELT 1X6SHT 3/8"PLY	BS, 1st-exterior-1.5" lap joints felt paper, 15#, 2nd sheathing, 1x6, 3rd-diagonally laid studs, 2x4", 4th-16"O.C. gypsum, 3/8", 5th timbers, 5 5/8", 6th-interior-stacked 2x6"'s
WOOD/METAL COMPOSITES			
79	55	BS F SHT STD GYP PLY SM	BS, 1st-exterior-1.5" lap joints felt paper, 15#, 2nd sheathing, 1x6, 3rd-diagonally laid studs, 2x4", 4th-16" O.C. gypsum, 3/8", 5th plywood, 3/4", 6th sheet metal, 1/8", 7th-interior

REFERENCES

[1]Gayle Rivers, The War Against Terrorists, How to Win It (Briarcliff Manor, N.Y.: Stein and Day, 1986), p.1.

[2]Edward A. Lynch, "International Terrorism: The Search for a Policy," Terrorism, An International Journal, v9, No.1 (1987), p. 20.

[3]Neil C. Livingstone, "Democracy Under Attack," in Fighting Back, Winning the War Against Terrorism, eds. Neil Livingstone and Terrell Arnold (Lexington, MA: D.C. Heath & Co., 1986), p. 2.

[4]Lynch, p.28.

[5]Richard Clutterbuck, Living with Terrorism (New York: Arlington House, 1975), p. 75.

[6]Christine C. Ketcham and Harvey J. McGeorge II, "Terrorist Violence: Its Mechanics and Countermeasures" in Fighting Back, Winning the War Against Terrorism, pp. 27-28.

[7]Ketcham, pp. 30-32.

[8]Lynch, p. 42.

[9]Terrell E. Arnold and Neil C. Livingstone, "Fighting Back" in Fighting Back, Winning the War Against Terrorism, pp.245-246.

[10]James Berry Motley, "Target America: The Undeclared War" in Fighting Back, Winning the War Against Terrorism, p. 64.

[11]Donald G. Bruckner, "Security Systems Engineering, A Vital Military Construction Need," The Military Engineer, v79 (March/April 1987), p.85.

[12]Bruckner, p. 86.

[13]Embassy Concerns Raised," Engineering News-Record, v216, No. 11 (March 13, 1986), p10.

[14]Larry Green, "Combatting Terrorism, Designing the Shield," Consulting-Specifying Engineer, v78 (August 1986), p. 62.

[15]David R. Coltharp, "Designing Buildings Against Terrorists," The Military Engineer, v79 (August 1987), p.428.

[16]Naval Facilities Engineering Command, Design Guidelines for Physical Security of Fixed Land-Based Facilities (DM 13.1) (Alexandria VA: March, 1983), p. 115.

[17]DM 13.1, p. 119.

[18]Mark D. Buffkin, "Growing: the Art of Anti-terrorist Engineering," Navy Civil Engineer, v27 (Summer 1987), p. 7.

[19]Don T. Cherry, Total Facility Control (Boston, MA: Butterworth Publishers, 1986), pp. 159-169.

[20]Navy Civil Engineering Laboratory, Terrorist Vehicle Bomb Survivability Manual (Port Hueneme, CA:March 1986), p.6-2.

[21]DM 13.1, pp. 124-125.

[22]Cherry, pp. 106-107.

[23]John E. Cunningham, Security Electronics (Indianapolis, IN: Howard W. Sams & Co., 1983), pp. 46-51.

[24]Cherry, pp. 107-113.

[25]Naval Facilities Engineering Command, Commercial Intrusion Detection Systems (DM 13.02) (Alexandria, VA: Sept. 1986), p.1.

[26]Kenneth O. Gray, "Vehicle Access Control, Countermeasures Against Car-bomb Attacks," The Military Engineer, v79 (March/April 1987), p. 108.

[27]Terrorist Vehicle Bomb Survivability Manual, p. 3-7.

[28]Terrorist Vehicle Bomb Survivability Manual, p. 3-6.

[29]Peter Slavin and Nick Adde, "20 Years After Tet," The Navy Times, No. 16 (Febraury 1, 1988), p. 81.

[30] Terrorist Vehicle Bomb Survivability Manual, p. 3-10.

[31] Terrorist Vehicle Bomb Survivability Manual, p. 3-9.

[32] Gray, pp. 108-110.

[33] Terrorist Vehicle Bomb Survivability Manual, pp. 8-1 to 8-24.

[34] Terrorist Vehicle Bomb Survivability Manual, pp. 7-1 to 7-27.

[35] Marc S. Caspe and Andrei Reinhorn, "The Blast Barrier, A New Protection System," The Military Engineer, v79 (March/April 1987), p. 101.

[36] Caspe, pp. 102-103.

[37] DM 13.1, p. 281.

[38] Geral E. Meyers, "Blast-resistant Glazing," The Military Engineer, v78 (August 1986), p. 474.

[39] Randall R. Nason and John A. Milloy, "Facility Security, Remember the Power!" The Military Engineer, v79 (March/April 1987), pp. 92-95.

[40] Green, p. 64.

BIBLIOGRAPHY

Bruckner, Donald G. "Security Systems Engineering, A Vital Military Construction Need." The Military Engineer, v79, No. 513 (March/April 1987), 84-87.

Buffkin, Marc D. "Growing: the Art of Anti-terrorist Engineering." Navy Civil Engineer, v27, No. 1 (Summer 1987), 6-8.

Caspe, Marc S. and Andrei M. Reinhorn. "The Blast Barrier, A New Protection System." The Military Engineer, v79, No. 513 (March/April 1987), 100-105.

Cherry, Don T. Total Facility Control. Boston, MA: Butterworth Publishers, 1986.

Clutterbuck, Richard. Living With Terrorism. New York: Arlington House Publishers, 1975.

Coltharp, David R. "Designing Buildings Against Terrorists." The Military Engineer, v79, No. 516 (August 1987), 427-429.

Cunningham, John E. Security Electronics. Indianapolis, IN: Howard W. Sams & Co., Inc., 1983.

"Embassy Concerns Raised." Engineering News Record, v216, No. 11 (March 13, 1986), pp. 10-11.

Gray, Kenneth O. "Vehicle Access Control, Countermeasures Against Car-bomb Attacks." The Military Engineer, v79, No. 513 (March/April 1987), 108-114.

Green, Larry. "Combatting Terrorism, Designing the Shield-Part II." Consulting-Specifying Engineer, v1, No. 2 (February 1987), 62-67.

Livingstone, Neil C. and Terrell E. Arnold, eds. Fighting Back, Winning the War Against Terrorism. Lexington, MA: D.C. Heath and Co., 1986.

Lynch, Edward A. "International Terrorism: The Search for a Policy." Terrorism, An International Journal, v9, No. 1 (1987), 1-86.

Meyers, Gerald E. "Blast-resistant Glazing." The Military Engineer, v78, No. 509 (August 1986), 473-474.

Montana, Patrick J. and George S. Roukis, eds. Managing Terrorism, Strategies for the Corporate Executive. Wesport, CT: Quorum Books, 1983.

Nason, Randall R. and John A. Milloy. "Facility Security, Remember the Power!" The Military Engineer, v79, No. 513 (March/April 1987), 92-95.

Naval Facilities Engineering Command. Commercial Intrusion Detection Systems (IDS) (DM 13.1). September 1986.

Naval Civil Engineering Laboratory. Navy Physical Security Equipment Manual. Department of the Navy, July 1986.

Naval Civil Engineering Laboratory. Terrorist Vehicle Bomb Survivability Manaul (Vehicle Barriers). Department of the Navy, March 1986.

Naval Facilities Engineering Command. Design Guidelines For Physical Security of Fixed Land-Based Facilities (DM 13.1). March, 1983.

Naval Facilities Engineering Command. Utility Systems Vulnerability Guide (P-1023). December, 1986.

Netamyohue, Benjamin. Terrorism, How the West Can Win. New York: Farrar, Strauss and Grioux, 1986.

New York State Report of the Policy Study Group on Terrorism. The Criminal Justice Institute, Nov. 1985.

Pickett, Ted L. and Steven J. Gunderson. "Improving Physical Security." The Military Engineer, v78, No. 509 (August 1986), 478-480.

Rivers, Gayle. The War Against the Terrorists, How To Win It. Briarcliff Manor, NY: Stein and Day, 1986.